



# THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office

*December 01, 2004*

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: 60/483,277  
FILING DATE: *June 25, 2003*  
RELATED PCT APPLICATION NUMBER: *PCT/US04/20562*

Certified by



Jon W Dudas

Acting Under Secretary of Commerce  
for Intellectual Property  
and Acting Director of the U.S.  
Patent and Trademark Office

# PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No.

EU245163327 US

PTO  
17507 U.S. PTO  
607 83277

06/25/03

## INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Lance M.	Cottrell	San Diego, California
James A	Reynolds	Carlsbad, California
Darya	Mazandarany	San Diego, California

☒ Additional inventors are being named on the 1 separately numbered sheets attached hereto

## TITLE OF THE INVENTION (500 characters max)

A MULTIPLE PLATFORM NETWORK PRIVACY SYSTEM

Direct all correspondence to:

### CORRESPONDENCE ADDRESS

☐ Customer Number

OR

Type Customer Number here

Place Customer Number  
Bar Code Label here

☒ Firm or  
Individual Name

Francisco A. Rubio-Campos

Address The Eclipse Group

Address 26895 Aliso Creek Road, Suite B-104

City Aliso Viejo

State

CA

ZIP

92656

Country USA

Telephone

949-448-9410

Fax

714-948-8903

## ENCLOSED APPLICATION PARTS (check all that apply)

☒ Specification Number of Pages

74

☐ CD(s), Number

☐ Drawing(s) Number of Sheets

☐ Other (specify)

☐ Application Data Sheet. See 37 CFR 1.76

## METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.

☒ A check or money order is enclosed to cover the filing fees

☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:

502542

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE  
AMOUNT (\$)

\$80.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE

Date 06/25/2003

TYPED or PRINTED NAME Francisco A. Rubio-Campos

TELEPHONE (949) 448-9410

REGISTRATION NO.

(if appropriate)

Docket Number:

45,358

IF03001USV

## USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant

16076 U.S. PRO

Approved for use through 04/30/2003. OMB 0651-0032  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$ 80.00

## Complete if Known

Application Number	Unknown
Filing Date	June 25, 2003
First Named Inventor	Lance M. Cottrell et al.
Examiner Name	Not applicable
Art Unit	Unassigned
Attorney Docket No.	IF03001USV

## METHOD OF PAYMENT (check all that apply)

☐ Check ☒ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit  
Account  
Number  
Deposit  
Account  
Name

502542

The Eclipse Group

The Director is authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☒ Credit any overpayments  
☐ Charge any additional fee(s) during the pendency of this application  
☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

## FEE CALCULATION

### 1. BASIC FILING FEE

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
1001 750	2001 375	Utility filing fee	
1002 330	2002 165	Design filing fee	
1003 520	2003 260	Plant filing fee	
1004 750	2004 375	Reissue filing fee	
1005 160	2005 80	Provisional filing fee	80.00

SUBTOTAL (1) (\$ 80.00

### 2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

Total Claims	Extra Claims	Fee from below	Fee Paid
Independent	-20** =	X	
Multiple Dependent	-3** =	X	

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description
1202 18	2202 9	Claims in excess of 20
1201 84	2201 42	Independent claims in excess of 3
1203 280	2203 140	Multiple dependent claim, if not paid
1204 84	2204 42	** Reissue independent claims over original patent
1205 18	2205 9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) (\$ 0.00

\*\*or number previously paid, if greater; For Reissues, see above

## FEE CALCULATION (continued)

### 3. ADDITIONAL FEES

Large Entity Small Entity

Fee Code (\$)	Fee Code (\$)	Fee Description	Fee Paid
1051 130	2051 65	Surcharge - late filing fee or oath	
1052 50	2052 25	Surcharge - late provisional filing fee or cover sheet	
1053 130	1053 130	Non-English specification	
1812 2,520	1812 2,520	For filing a request for ex parte reexamination	
1804 920*	1804 920*	Requesting publication of SIR prior to Examiner action	
1805 1,840*	1805 1,840*	Requesting publication of SIR after Examiner action	
1251 110	2251 55	Extension for reply within first month	
1252 410	2252 205	Extension for reply within second month	
1253 930	2253 465	Extension for reply within third month	
1254 1,450	2254 725	Extension for reply within fourth month	
1255 1,970	2255 985	Extension for reply within fifth month	
1401 320	2401 160	Notice of Appeal	
1402 320	2402 160	Filing a brief in support of an appeal	
1403 280	2403 140	Request for oral hearing	
1451 1,510	1451 1,510	Petition to institute a public use proceeding	
1452 110	2452 55	Petition to revive - unavoidable	
1453 1,300	2453 650	Petition to revive - unintentional	
1501 1,300	2501 650	Utility issue fee (or reissue)	
1502 470	2502 235	Design issue fee	
1503 630	2503 315	Plant issue fee	
1460 130	1460 130	Petitions to the Commissioner	
1807 50	1807 50	Processing fee under 37 CFR 1.17(q)	
1808 180	1808 180	Submission of Information Disclosure Stmt	
8021 40	8021 40	Recording each patent assignment per property (times number of properties)	
1809 750	2809 375	Filing a submission after final rejection (37 CFR 1.129(a))	
1810 750	2810 375	For each additional invention to be examined (37 CFR 1.129(b))	
1801 750	2801 375	Request for Continued Examination (RCE)	
1802 900	1802 900	Request for expedited examination of a design application	

Other fee (specify)

\*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$ 0.00

## SUBMITTED BY

Name (Print/Type) Francisco A. Rubio-Campos

Registration No. 45,358  
(Attorney/Agent)

(Complete if applicable)

Telephone 949-448-9410

Signature

Date June 25, 2003

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

# PROVISIONAL APPLICATION COVER SHEET

## Additional Page

PTO/SB/16 (02-01)

Approved for use through 10/31/2002. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Docket Number	IF03001USV
---------------	------------

INVENTOR(S)/APPLICANT(S)		
Given Name (first and middle (if any))	Family or Surname	Residence (City and either State or Foreign Country)
Steve Walsh	Walsh	Tara QLD 4421, Australia
Peleus Uhley	Uhley	Alameda, California
Gene Nelson	Nelson	Spring Valley, California
Robert Torres	Torres	Chula Vista, California

Number   2   of   2  

**WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

## Table of Contents      Error! Bookmark not defined.

1. Introduction .....	2
How to read this document .....	<b>Error! Bookmark not defined.</b>
Objective .....	2
2. Scope .....	2
1.1 Product Overview .....	2
3. Product Features .....	2
4. Modules .....	3
4.1. AnonPro Web Server Startup Wizard Support Script .....	3
4.1.1. Overview .....	3
4.1.2. Key Validation .....	3
4.1.3. Account Creation .....	4
4.1.4. Script Input: .....	5
4.1.5. Script Output: .....	6
4.1.6. XML Format .....	6
5. System .....	9
5.1. Platform .....	9
5.2. Languages .....	9
Reliability / Redundancy / Scalability .....	9
Security .....	9
1.2 Product Integration Interface .....	9
API Integration .....	10
3 <sup>rd</sup> Party Data mapping .....	10
Common Components .....	10
Overview .....	10
Component 1 .....	10
Error Handling / Logging .....	10
Appendix A - Reports .....	<b>Error! Bookmark not defined.</b>

# **1. Introduction**

## **Objective**

The objective of this functional specification document is to help describe the functional features of a product solution.

# **2. Scope**

This document is intended to provide a high level description of the Web-Server functionality for the AnonPro release.

## **Product Overview**

This section describes the product from a high level perspective.  
Please include a diagram to help in the overview.

# **3. Product Features**

This section lists a summarized listing of the features as listed in the business requirements document and or conceptual overview.

## 4. Modules

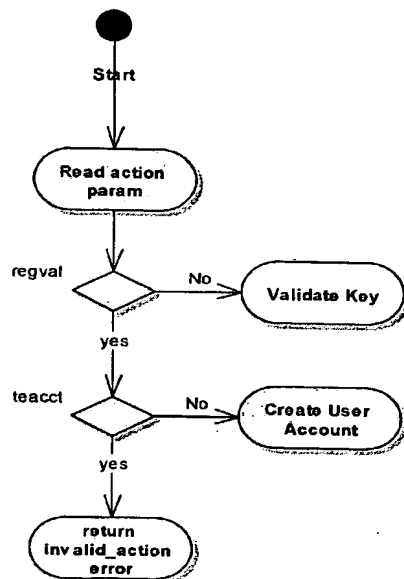
This section lists a summarized listing of the modules required for the AnonPro Web-Server development.

### 4.1. AnonPro Web Server Startup Wizard Support Script

#### 4.1.1. Overview

This project will be a CGI script written in PERL. Its purpose is to interface with the AnonPro client application Startup Wizard Module. The AnonPro client will be making an HTTPS posts to this script when the Startup Wizard Module is called. This script will be required to determine the action to take based upon an "action" parameter. The two defined actions are: Key Validation and Account Creation.

The script will return all results in XML format.

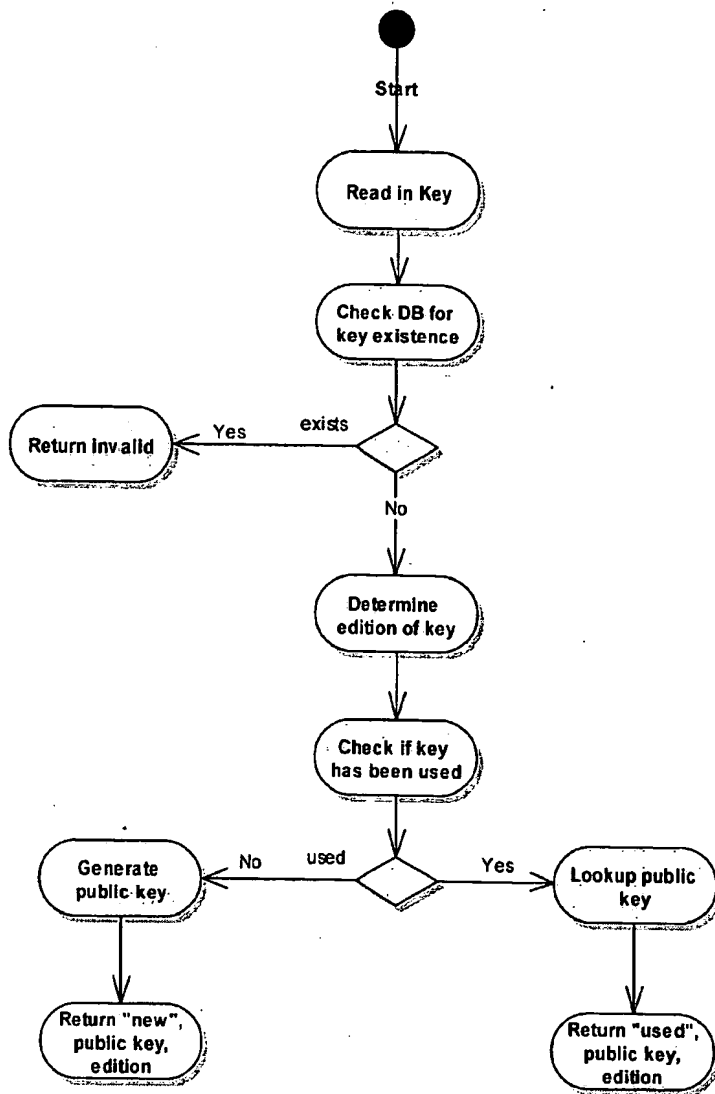


#### 4.1.2. Key Validation

When the AnonPro Web Server Startup Wizard Support Script receives an action parameter equal to "regval" it will perform Key Validation.

The first step of key validation is reading in the registration key from the "regkey" parameter. The script will reference the Anonymizer database to find out if this key exists in the registration key table. Existence in this table will determine that this is a valid registration key. If the key exists in the database the edition that is associated with it will be retrieved as well.

If this key has been previously used, it will lookup the public key that is associated with the registration key. It will then return the edition and public key to the client with the status of "used". If the key has not been previously used the script will generate a public key and store it in the database. It will then return the edition, public key, and a status of "new".



#### 4.1.3. Account Creation

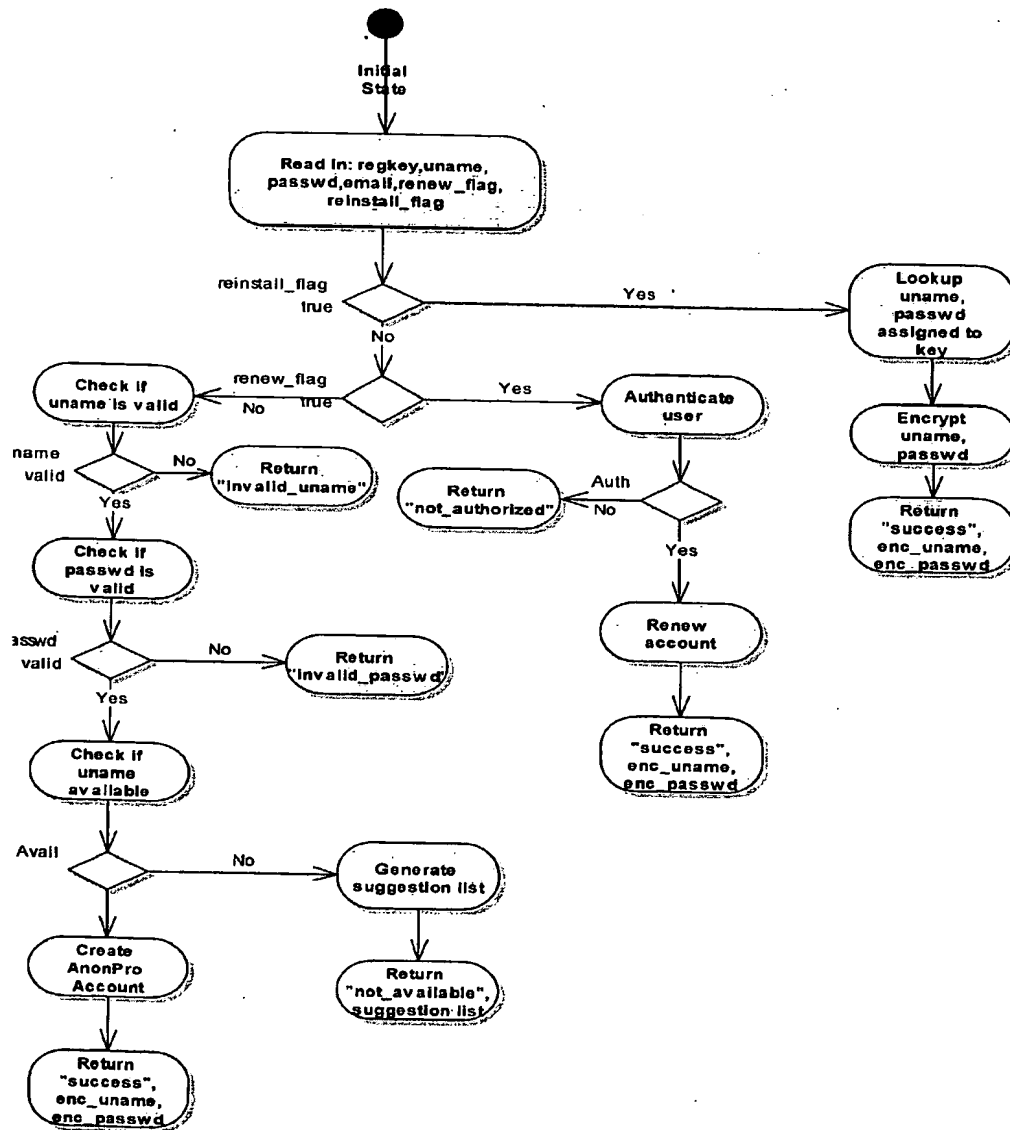
The account creation section will handle the creation, renewal, or reinstallation of the user's account. We will look at each of these scenarios separately.

Account creation is performed when an unused key is passed in with a valid and available username and password. The user will be inserted into the necessary tables in order to allow the user to use the AnonPro service.



Account renewal is performed when an unused key is passed in with the username and password of an existing user. The user's account is then updated to reflect the upgrade in service determined by the registration key.

Account reinstallation is performed when the user is not creating a new account or upgrading/renewing an existing account, but is merely trying to activate an installation of the AnonPro client.



#### 4.1.4. Script Input:

Universal:

Action = "regval" || "createacct"  
Regkey = <KEY>

Action Dependent:

Key Validation

None

Account Creation

Uname = string

Passwd = string

Email = string

Renew = 0 || 1

Reinstall = 0 || 1

#### 4.1.5. Script Output:

Key Validation:

Keystatus = "invalid" || "used" || "new"

Publickey = <Public Key>

Edition = string

Account Creation:

Account\_status = "invalid\_uname" || "invalid\_passwd" || "not\_authorized" || "not\_available" || "success"

uname = username

Enc\_passwd = encrypted password

Suggestion\_list = 1 or more suggestions for username

#### 4.1.6. XML Format

```
<root>
<regval>
  <keystatus>invalid||used||new</keystatus>
  <publickey>public key generated by server</publickey>
  <edition>ProductType</edition>
</regval>
<createacct>

<account_status>invalid_uname||invalid_passwd||not_authorized||not_avai
lable
||success</createacct>
<suggestion_list>
  <suggestion>uname suggestion</suggestion>
</suggestion_list>
<uname>user name</uname>
<enc_passwd>encrypted passwd</enc_passwd>
```

```
</createacct>  
<error>invalid_action|none</error>  
</root>
```

## 4.2. AnonPro Web-Server Logon/Authentication Module

The AnonPro Web Server Login Script will handle user authentication for the AnonPro client. The AnonPro client will make a silent HTTPS post to the Login Script. In this post the AnonPro client will pass in the username and password of the user to be authenticated. This script will determine the status of the user and set the necessary cookies in order for the user to be able to use the AnonPro service. The following paragraphs will outline the complete procedure.

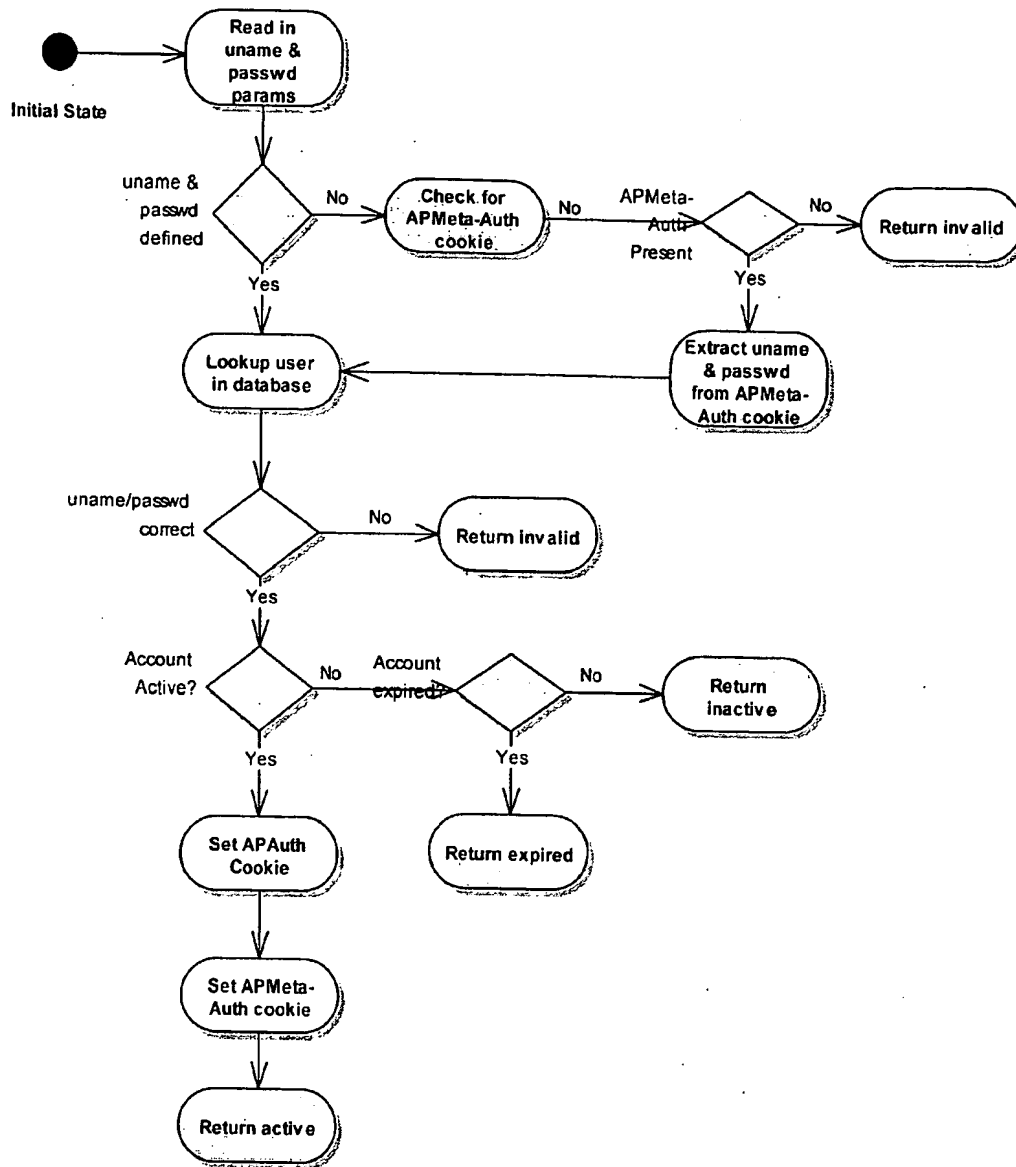
First the script checks to make sure the uname and passwd parameters have been passed in. If they are not passed in, it checks for the existence of an APMeta-Auth cookie. The username and password would then be extracted from the APMeta-Auth cookie and the script would proceed as normal. In the event that the username and password are not passed in and there is no APMeta-Auth cookie, the script will return an "invalid" status and exit.

The script then connects to the Anonymizer database and searches for a user with the given username and password. If a user is not found with the given information the script will return a status of "invalid". If the user is found, the script then checks to see if the user has an active AnonPro account. If the user does not have an AnonPro account or has an expired AnonPro account the script will return the status of "expired" (When the AnonPro client receives an "expired" status it should open a browser window and proceed to the URL contained in the Signup\_URL registry entry.). If the user owns an account that is not expired for some other reason is not active, the script will return a status of "inactive".

If it has been determined that the user has an active AnonPro account it will proceed in setting the necessary authorization cookies. The authorization cookies that the Login Script will set are the APAuth cookie and the APMeta-Auth cookie.

The APAuth cookie is what the AnonPro Proxy Servers will check in order to authenticate the user. It has a two hour lifetime. It contains the type of service of the user's account, the encrypted username, the timestamp for expiration (epoch time), and a hash which verifies the authenticity of the cookie.

The APMeta-Auth cookie is designed to allow the AnonPro Proxy servers the ability to redirect to the Login Script and receive authentication without interaction with the AnonPro client. The APMeta-Auth cookie contains the encrypted username and the uid (user id) of the user.



#### **4.2.1. APAuth Cookie**

```
<APAuth>
  <tos>type of service</tos>
  <uname>encrypted username</uname>
  <expires>unix timestamp for expiration</expires>
  <hash>hash of: secret string + tos + uname + expires +
secret string</hash>
</APAuth>
```

#### **4.2.2. APMeta-Auth Cookie**

```
<APMeta-Auth>
  <uname>encrypted uname</uname>
  <uid>user id</uid>
</APMeta-Auth>
```

## **5. System**

### **5.1. Platform**

This will need to run on Linux using Apache.

### **5.2. Languages**

This portion is language independent.

### **Reliability / Redundancy / Scalability**

#### **Scalability**

This product only needs to be able to support the maximum number of connections we expect the client to initiate (1 machine only).

#### **Reliability / Redundancy**

### **Security**

### **Product Integration Interface**

This section describes the <product> interface functionality.

## **Overview**

This section gives an overview of the interface components.

### ***API Integration***

### ***3<sup>rd</sup> Party Data mapping***

## **Common Components**

### ***Overview***

The common components are those components that can be used by multiple systems. They represent those infrastructure components necessary to transmit a message from one queue (either client or server side) to another queue.

### ***Component 1***

### ***Error Handling / Logging***

Error handling and logging are an important part to any system.

#### **Error Handling**

The SSL Server should behave similarly to any production web server with respect to how it handles its errors.

## Table of Contents

Table of Contents.....	11
1.1 Introduction.....	11
How to read this document.....	11
Objective.....	11
1.2 Scope.....	12
1.3 Product Overview.....	12
1.4 Product Features.....	12
Full Time SSL.....	12
1.5 Modules.....	12
Client Hooks.....	12
Client SSL Server.....	12
1.6 Architecture.....	15
1.7 System.....	16
Platform.....	16
Languages.....	16
Reliability / Redundancy / Scalability.....	17
Security.....	17
1.8 Product Integration Interface.....	17
API Integration.....	17
3 <sup>rd</sup> Party Data mapping.....	19
Common Components.....	19
Overview.....	19
Component 1.....	19
Error Handling / Logging.....	19
Glossary.....	<b>Error! Bookmark not defined.</b>
2 Product Acronyms.....	<b>Error! Bookmark not defined.</b>
3 AnonPro Terms.....	<b>Error! Bookmark not defined.</b>
Appendix A - Reports.....	<b>Error! Bookmark not defined.</b>

## 1 Introduction

### How to read this document

*Because this document is not yet finalized, you will also see some notes and comments interspersed with actual requirements. You can recognize comment text by its appearance in Times New Roman italicized font. This usually indicates some feedback is necessary from other departments or Project Stakeholders before the requirements can be completed.*

### Objective

The objective of this functional specification document is to help describe the functional features of a product solution.

## **2 Scope**

This document is intended to provide a high level description of the SSL functionality for the AnonPro release.

## **3 Product Overview**

This section describes the product from a high level perspective. Please include a diagram to help in the overview.

## **4 Product Features**

This section lists a summarized listing of the features as listed in the business requirements document and or conceptual overview.

### **Full Time SSL**

Full time SSL will enable users of the client to connect securely to the proxy if they are using any of the http protocols such as <http://www.yahoo.com> or <https://www.yahoo.com>. We benefit in two ways from this module one we are able to provide a secure means of communication with our proxy so we don't introduce any more threats. Two we effectively implement a man in the middle attack allowing us to seamlessly filter the users content for them even if they are browsing secure sites.

## **5 Modules**

### **Client Hooks**

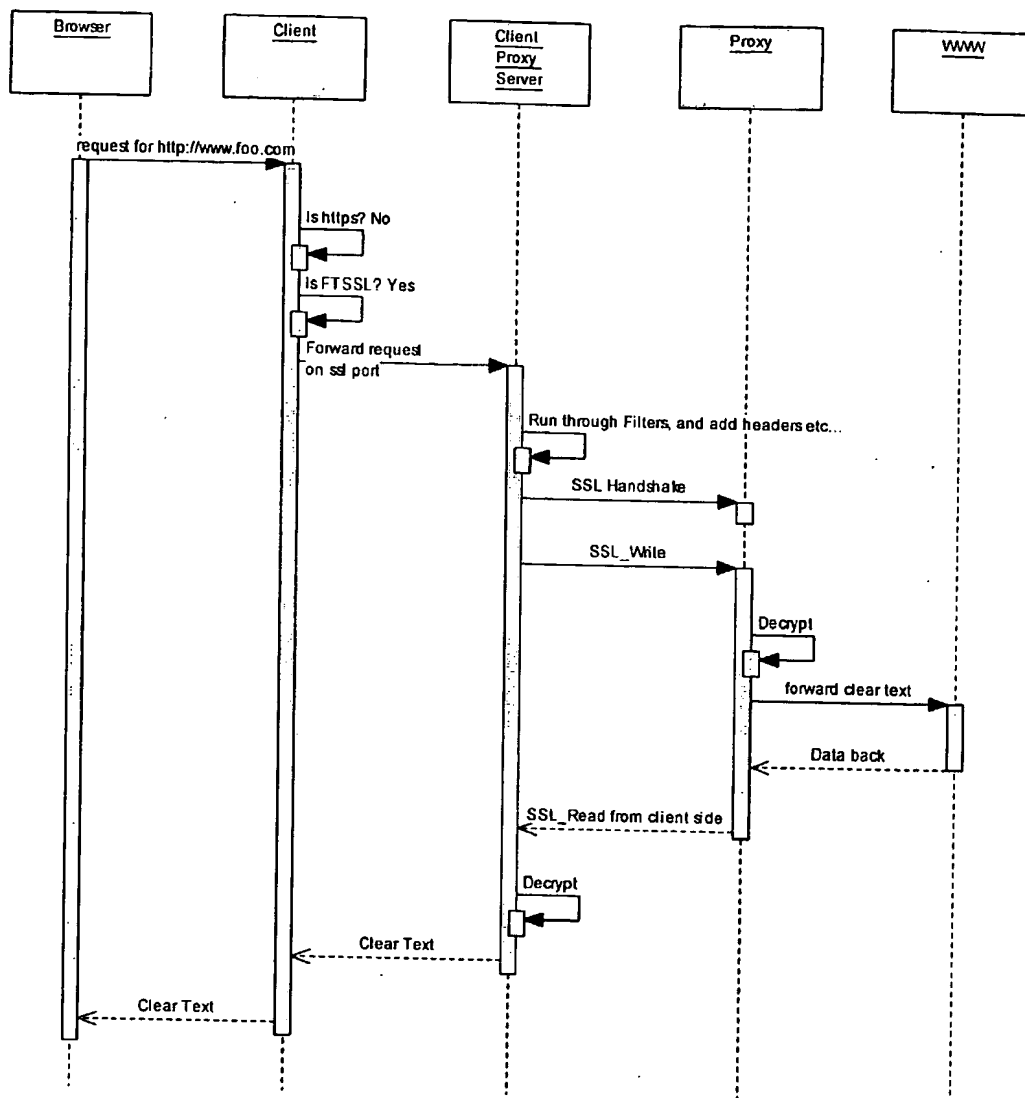
The authors of the client code will need to provide hooks to redirect traffic to the client side Proxy Server (to be described next). That server will be a fully functional web proxy that will process the https connection using the SSL module.

### **SSL Module**

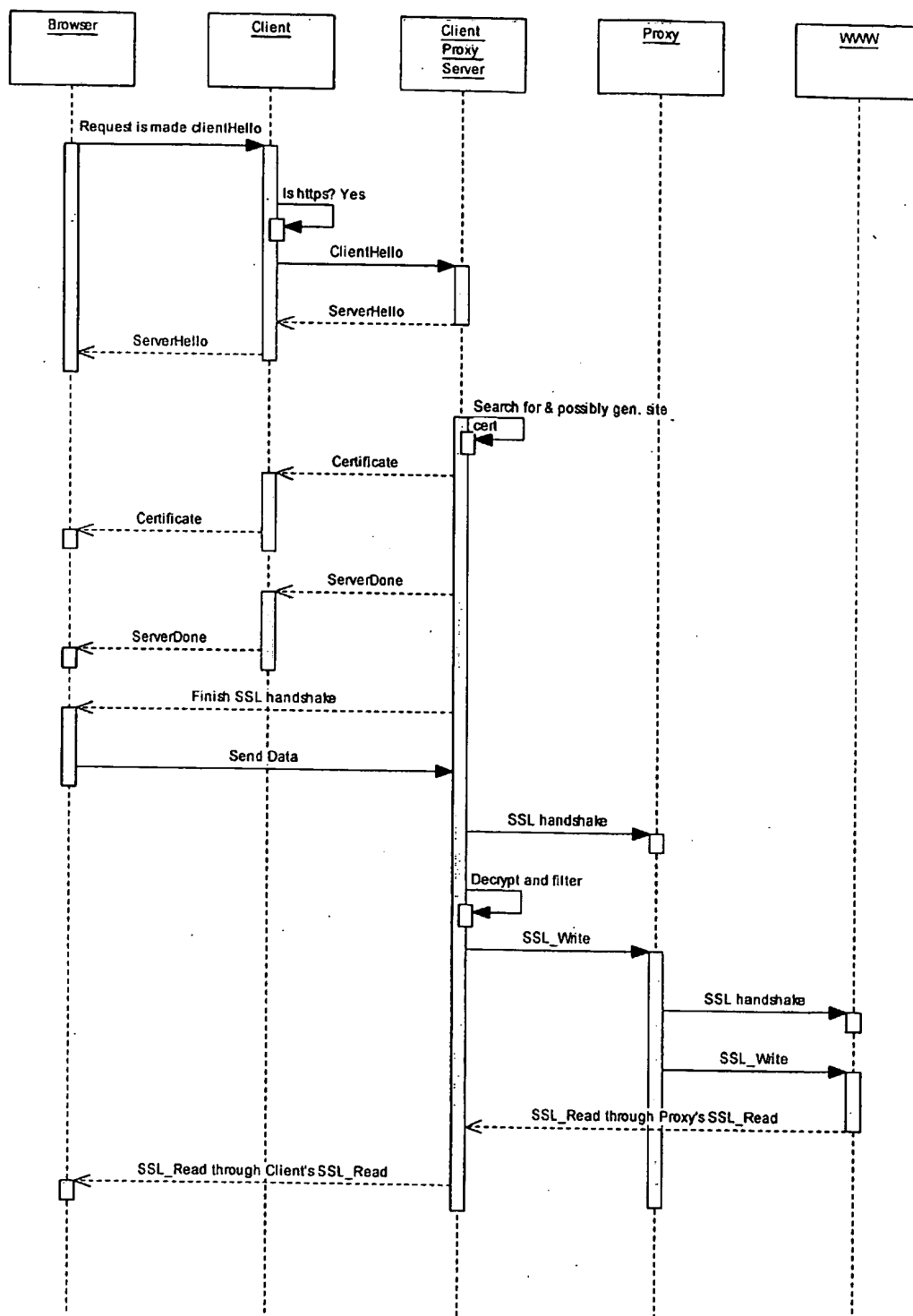
This Module will be called by the client proxy server when it receives an https connection. This can happen in two ways:

1. HTTP request Full Time SSL (FTSSL) on.





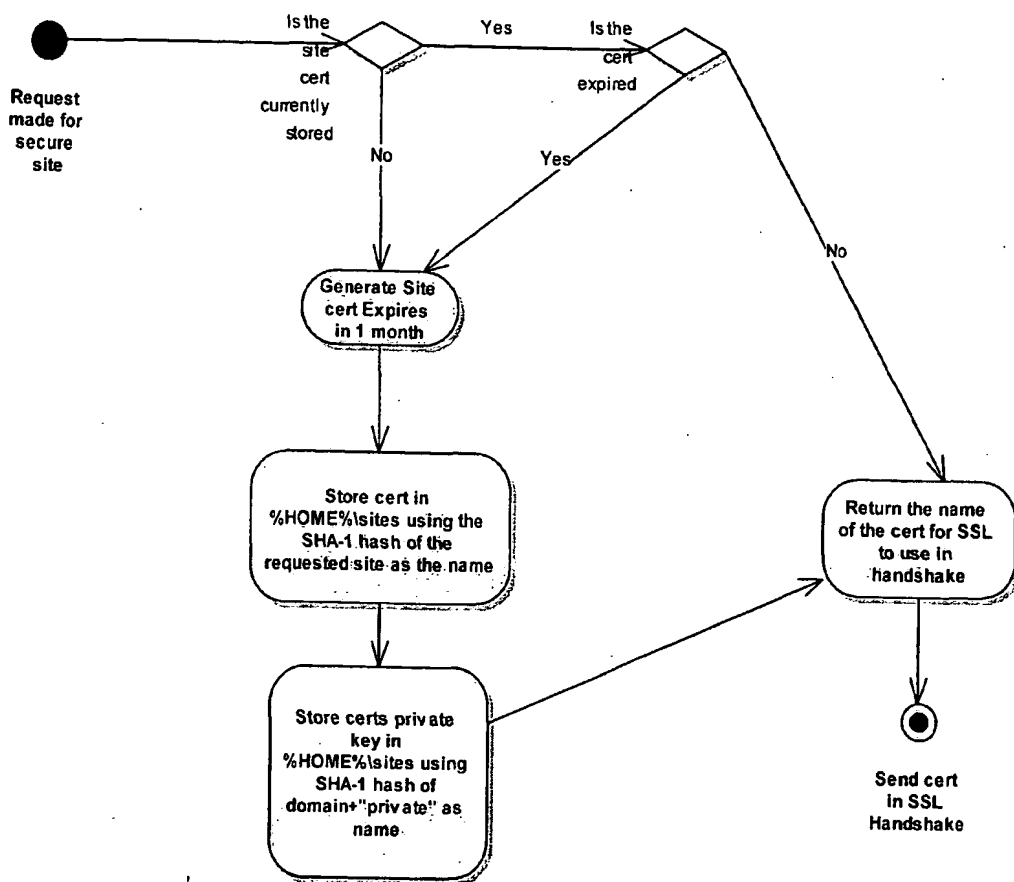
## 1. Requests made using SSL (HTTPS)



## 6 Architecture

The Client hooks module will simply be a placeholder for calls and callbacks but the Client Proxy Server will need to be a fully functional server. This means that it will have to listen on two ports for incoming secure as well as insecure connections and spawning a new thread to handle each connection. When the client is installed the User CA keys must be generated, also the Public User CA key needs to be installed in the browser preferably automatically but if this isn't possible we must provide instructions on how to do it manually. We will be using a universal site key to be signed by the User's Secret CA key to forge the authentication of the secure site. For security reasons we will spawn a background thread on startup to generate a new key and swap with the universal site key after it has been generated.

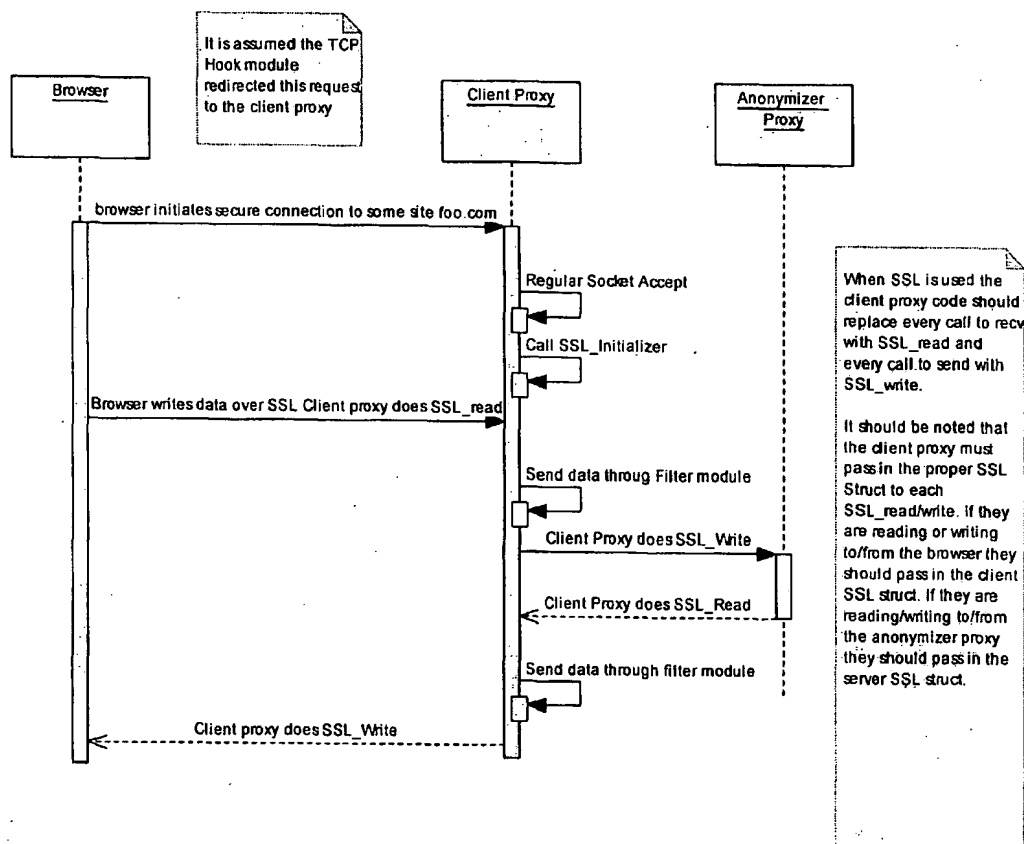
This section will explain how we assume the identity of the secure server the browser wishes to connect to.



When a request comes in for a secure site we must check to see if we have the site cert to return in the SSL handshake. We will check a table containing the file names of our disk cache located in HOME/sites where home is the registry entry for the program home. To store the certificates we will use a SHA-1 hash of the server they are representing. If we cannot find the certificate in our cache we must generate one for that site using our universal site certificate and the User CA Secret Key. Once generated this will be stored in the cache in the same manner.

After all of the above is completed we can finish the SSL handshake and begin the man in the middle attack. Essentially what we will be doing is decoding the SSL records on the client proxy server redirecting them through the filtering code and then doing an SSL\_Write to the anonymizer proxy. A similar flow is used when reading data from the anonymizer proxy we do an SSL\_Read giving us the clear text that was sent. Then send it though the filtering code. Finally we will do an SSL\_Write to the client, which will return it to the browser.

The sequence of events on the Client proxy is as follows. The TCP hook has redirected the browser request to us, we call the regular socket accept and make a call to SSL\_Initialize. The client proxy SSL handler will make calls to SSL\_read/write instead of the standard recv and send calls.



## 7 System

### Platform

This will need to run on all versions of windows the client will be supported on (XP, 2000, 98).

### Languages

This portion is language independent.

## **Reliability / Redundancy / Scalability**

### **Scalability**

This product only needs to be able to support the maximum number of connections we expect the client to initiate (1 machine only).

### **Reliability / Redundancy**

The Client Proxy server should be very reliable because we cannot have multiple servers listening on the same port we cannot have more than one on each client.

### **Security**

In order to prevent vulnerabilities in the system the server should do some form of client authentication to make sure other applications or even machines are trying to use the client proxy server.

## **8 Product Integration Interface**

This section describes the <product> interface functionality.

### **Overview**

This section gives an overview of the interface components.

### ***API Integration***

```
int SSL_Initialize(SSL *client, SSL *server, int browser_sock_descriptor, char
*destination_domain_name)
```

This will be the function to call before handling an SSL connection. It will create the SSL\_CTX and SSL structures for you and negotiate the SSL handshakes with the browser and the Anonymizer proxy.

#### **Parameters:**

- client – [out] SSL structure for communications between the browser and the client proxy.
- server – [out] SSL structure for communications between the client proxy and the anonymizer proxy.
- browser\_sock\_descriptor – [in] Socket descriptor used to associate the socket with the SSL connection.
- destination\_domain\_name – [in] Name of the destination the browser was attempting to connect to used to provide the proper site certificate to the

browser.

Return value – 1 on success, negative error code on failure.

Int SSL\_write (SSL \*info, const void \*buff, int len)

This is the OpenSSL function to call when you would like to write data to the browser (client), or server (anonymizer proxy) over the SSL connection established by SSL\_Initialize.

Parameters:

- client – [in] SSL structure used for communication (ex client or server from SSL\_Initialize).
- buff – [in] data buffer to write to the client.
- len – [in] number of bytes to write from the buffer.

Return value – the number of bytes written, 0 if it was unsuccessful or less than 0 if there is an error code.

Int SSL\_read(SSL \*client, const void \*buff, int len)

This is the OpenSSL function to call when you would like to read data from the browser (client) or server(anonymizer proxy) over the SSL connection established by SSL\_Initialize. It should be noted that since SSL data is sent in records and buffered this call may not return the maximum number of bytes and may need to be called repeatedly to receive all the data from the server.

Parameters:

- client – [in] SSL structure used for communication(ex client or server from SSL\_Initialize).
- buff – [in] data buffer to populate.
- len – [in] max number of bytes to read into the buffer.

Return value – the number of bytes written, 0 if it was unsuccessful or less than 0 if there is an error code.

int filter\_buffer(void \*\*buff, DWORD bitmask)

This is the function that will take the data received and run it through the filtergate filters in some fashion.

Parameters:

- buff – [in/out] data buffer to filter.
- bitmask – [in] bitmask of the filters to run.

## ***3<sup>rd</sup> Party Data mapping***

### **Common Components**

#### ***Overview***

The common components are those components that can be used by multiple systems. They represent those infrastructure components necessary to transmit a message from one queue (either client or server side) to another queue.

#### ***Component 1***

#### ***Error Handling / Logging***

Error handling and logging are an important part to any system.

#### **Error Handling**

The SSL Server should behave similarly to any production web server with respect to how it handles its errors.

## 9 Table of Contents

1. Introduction .....	21
2. Scope .....	21
2.1. Product Overview .....	21
3. AnonPro Project Details .....	21
3.1. Project Team and Responsibilities .....	22
3.2. Deliverables .....	22
3.3. BugTracking .....	23
3.4. QA Drops in between deliverables .....	23
4. AnonPro Client Module Architecture .....	23
4.1. General Architecture .....	23
4.2. Startup Wizard Module .....	23
4.3. Startup Module .....	26
4.4. Login/Authentication Module .....	28
4.5. Renew /Upgrade Module .....	29
4.6. TCP Hook module .....	30
4.7. Client Update Module .....	31
4.8. Client Proxy Module .....	32
4.9. Recently Visited Sites .....	38
4.10. GUI .....	39
5. System .....	64
Platform .....	64
5.1. Languages .....	64
5.2. Error Handling .....	65
5.3. Logging .....	65
5.4. Reliability / Redundancy .....	65
5.5. Secure Session .....	65
5.6. Username and Password .....	66
6. Reference Documents .....	66
7. Glossary .....	67
Product Acronyms .....	67
Appendix A – Data Structure Definitions .....	67
Preferences Bit Mask .....	67
APAuth Cookie .....	67
Meta-Auth Cookie .....	68
AnonPro cookie .....	68
Blocked/Trusted/Protected List .....	68
Server List .....	68
Update list .....	69
Account_Creation_URL return .....	69
Login_URL return .....	70
Appendix B – Registry Settings .....	70
Appendix C – Color RGB Matrix .....	73



## 6. Introduction

### How to read this document

*Because this document is not yet finalized, you will also see some notes and comments interspersed within the function specification. You can recognize comment text by its appearance in Times New Roman italicized font. This usually indicates some feedback is necessary from other departments or Project Stakeholders before the requirements can be completed.*

### Code Name

This project has been given the code name "AnonPro". This will not be the final name that the project is marketed as. All documentation and GUI components listed in this document, as "AnonPro" will be changed at a later date in time and therefore need to be programmed to allow easy changing at a later point in time.

### Objective

The objective of this functional specification document is to help describe the functional features of the AnonPro Client application.

## 7. Scope

### 7.1. Product Overview

This project builds on the features and functions of previous projects: Anonymizer 2.0, which uses the Proxy server, located at Anonymizer. Some components in the proxy server may need to be modified and at this point it is not known what the scope is.

It is important to note that the AnonPro 1.0 project will NOT be phasing out the Anonymizer 2.0 product - but rather will leverage the proxy server infrastructure as well as some of the existing functionality to work. AnonPro and Anonymizer 2.0 will work in parallel - independently of each other's product set. The Toolbar and Navbar will continue to be supported by Anonymizer. Nevertheless, if the user installs the AnonPro client, any previously installed Anonymizer toolbars will be uninstalled.

## 8. AnonPro Project Details

This project consists of many modules that have been split up to accommodate the areas of expertise and timeline. This document covers only the AnonPro Client portion of the project. There are 3 other components

that are not described in the document:

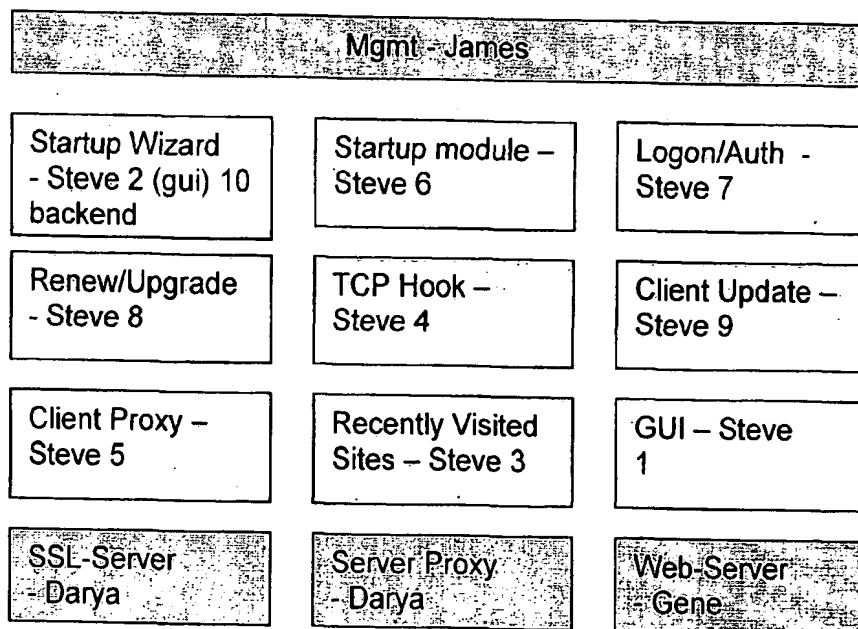
1. AnonPro SSL-Server
2. AnonPro Web-Server
3. AnonPro Server-Proxy

In addition, the AnonWasher project is running in parallel – but isn't really dependent on any of the components of this project.

### 8.1. Project Team and Responsibilities

This project is split into major components and assigned to the following teams:

Dev. Management	- James / Director of Engineering
AnonPro GUI Design	- Robert / Marketing Manager
AnonPro Client	- Steve Walsh (Outsource)
AnonPro Communication	- Steve Walsh (Outsource)
AnonPro Web Server	- Gene / Web-Server Engineer
AnonPro Proxy	- Darya / Proxy Engineer
AnonWasher	- Azi / AnonWasher Engineer
SSL-Server	- Darya / Proxy Engineer



### 8.2. Deliverables

The deliverables are identified as follows and correspond to the module sections as described in this document:

- 1<sup>st</sup> deliverable: gui, startup wizard gui
- 2<sup>nd</sup> deliverable: tcp hook, client proxy, recently visited sites

- 3<sup>rd</sup> deliverable: startup module, logn/auth, renew/upgrade, client update, startup wizard backend (needs a login to the web-server).

### 8.3. BugTracking

BugTracking will take place using Way to track bugs. Steve will require access to our Bugzilla.

### 8.4. QA Drops in between deliverables

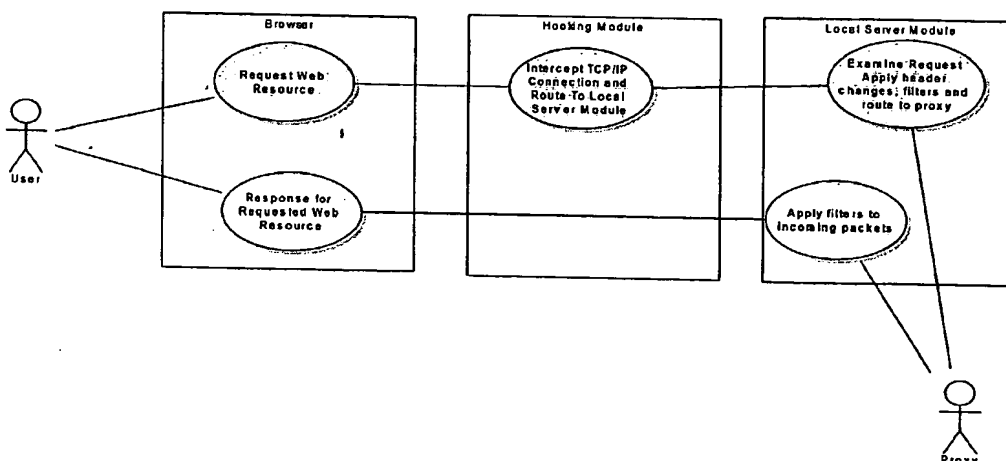
Between the deliverables, there will be QA drops that will be necessary to fix bugs that arose from the previous drop. Each drop will be scheduled on a case-by-case basis (depending on the severity and quantity of bugs).

## 9. AnonPro Client Module Architecture

Architecture and Description of all modules.

### 9.1. General Architecture

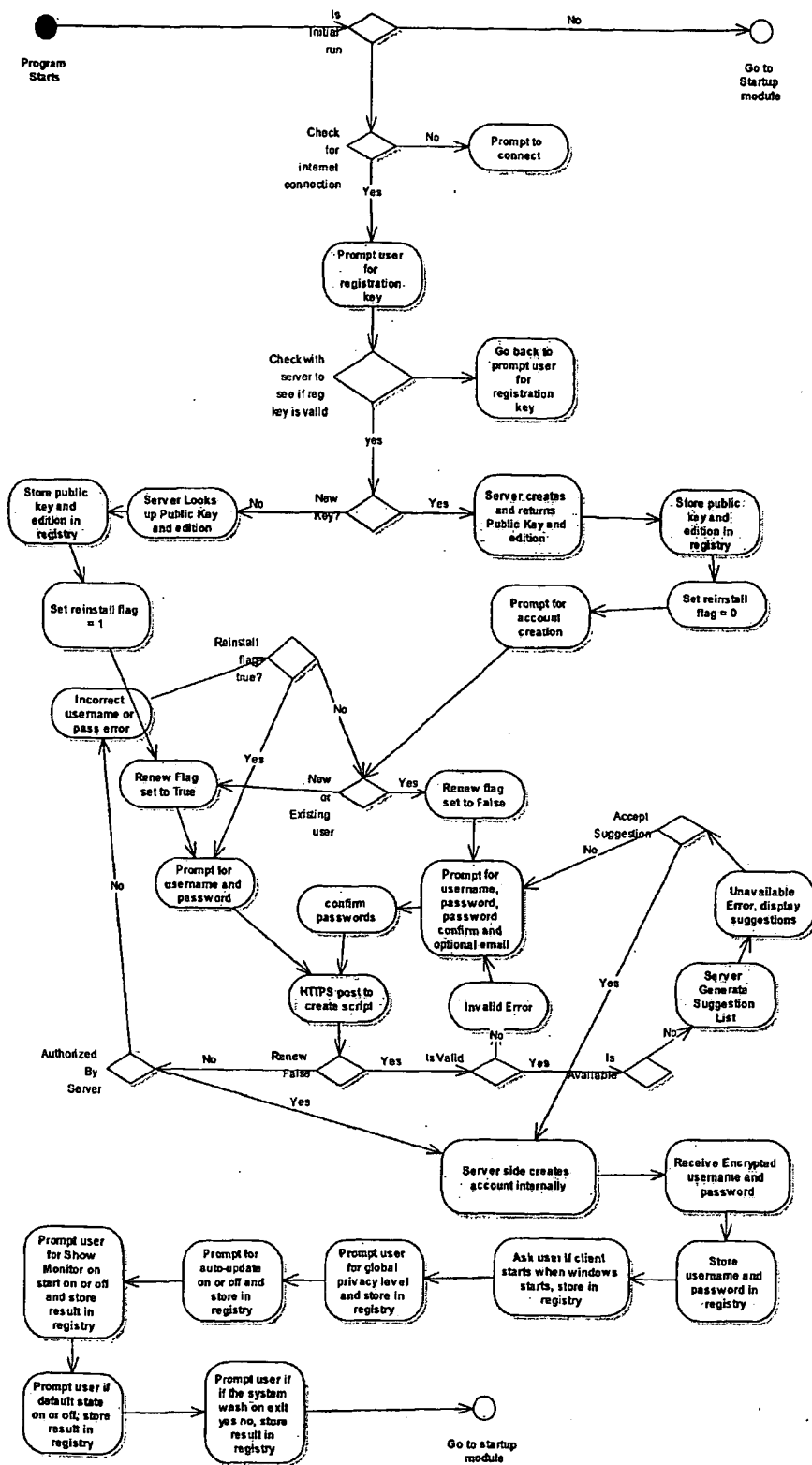
The main goal of this system is to shield the user from the various threats presented when using the Internet. To achieve this we must embed ourselves in the tcp layer of the system and route the client's data to a transparent proxy running on the client. The client proxy will determine what filters to apply based on the users settings and then forward the data to the anonymizer proxy to perform additional security measures. As a side note the location of the server cert will be known from the registry entry AnonPro\_Home\_Directory. The client will then need to go to AnonPro\_Home\_Directory\sites where the server cert is located and read it in. The server cert will be used to do silent SSL connections with the Web-Server to send usernames, passwords etc....



### 9.2. Startup Wizard Module

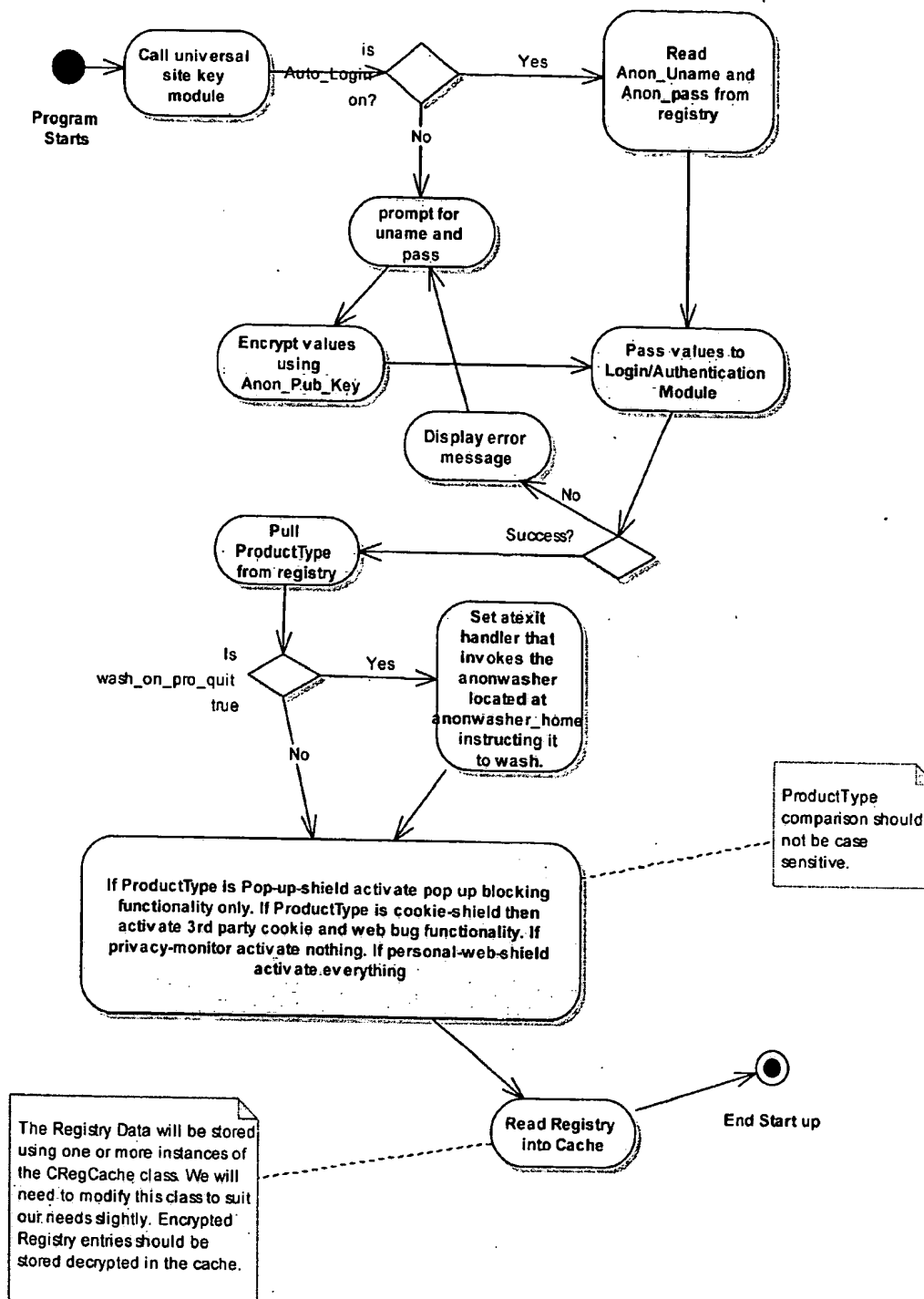
When the client is started, it is loaded into the system tray and displayed as an icon. Immediately

after that, the client checks to see if the client is being run for the first time (*Stored in the registry see Initial Execution*) if so the client startup wizard (REFERENCE SCREEN SHOT) is invoked. The wizard will check for an Internet connection (by checking the return value of a socket connect or another method if anyone can suggest one) and prompt the user to open one if no such connection is found. Next it will prompt the user to enter his/her registration key (26 characters hexadecimal with dashes retrieved from cd package or provided when software is downloaded) this will be posted to the registry value Account Creation URL with a query string "?action=regval&regcode=<registration code>" this will return a xml document Account Creation URL return. A return value of 0 means the key is invalid and a message should be displayed followed by reprompt for key otherwise the product edition is to be stored in the registry ( ProductType ) and the public key for the user will be stored in the registry ( Anon Pub Key ) and the user will start the account creation process. The wizard will ask the user if he/she is new or existing if they are existing they will be prompted for their username and password if they are a new user they will be prompted for their desired username, password, password confirmation and optional email address. The wizard will verify that the two passwords match throwing an error message if they don't then lookup the account creation URL (Account Creation URL) and do a https post to it passing in the user info as a query string if renew flag is 0 querystring = "?action=createacct&renewflag=<renewflag>&reinstallflag=<reinstallflag>&uname=<username>&passwd=<password>&email=<email>" where <renewflag> is either 0 for new user or 1 for existing and <reinstallflag> is 0 for unused registration key and 1 for a used registration key. This post will return an XML document Account Creation URL return. The wizard will then prompt the user if he/she would like the system to start when windows starts (or they login) if they choose yes we must create the Run when win starts registry entry. We must also prompt for the global security level(7 settings on the slider) after the user picks one, we must write the corresponding bitmask into the Security Level registry entry. We must also prompt for auto update on or off and write that into the Auto update registry entry. Next we must prompt to see if we should show the privacy monitor on startup, this should be stored in the Show floater registry entry. Now we need to prompt the user to see if the default state of the system is on or off and store the result in the Default state registry entry. Finally we must prompt the user to see if we should run the AnonWahser on exit or not and the result must be stored in the Wash on Pro Quit registry entry. If no error is returned the wizard must set the Initial Execution flag to false.



### 9.3. Startup Module

This module handles the flow of the client when it starts. First it will call the universal site key module then it will check the Auto\_login registry setting to see if it should prompt for the username and password. If Auto\_Login is enabled the Anon\_Uname and Anon\_Password will be passed to the Login/Authentication Module. If Auto\_Login is not enabled then we must use the Anon\_Pub\_Key to encrypt the username and password that the user entered and pass those values to the Login/Authentication Module. If the return value of the module is not success then we need to throw an error message and reprompt for the username and password. We must check the Wash\_on\_Pro\_Quit registry entry if its 1 we need to set a atexit handler that will call the AnonWasher executable with the command to wash now. The AnonWasher Executable will be located at AnonWasher\_Home and the parameter to pass in to invoke wash will be given. Otherwise we have success and we can read the registry into our cache.



Please note: Despite the diagram above - for this project, there will not be editions of AnonPro that will change the behavior or screens of AnonPro client. This functionality will be included in

later releases of AnonPro.

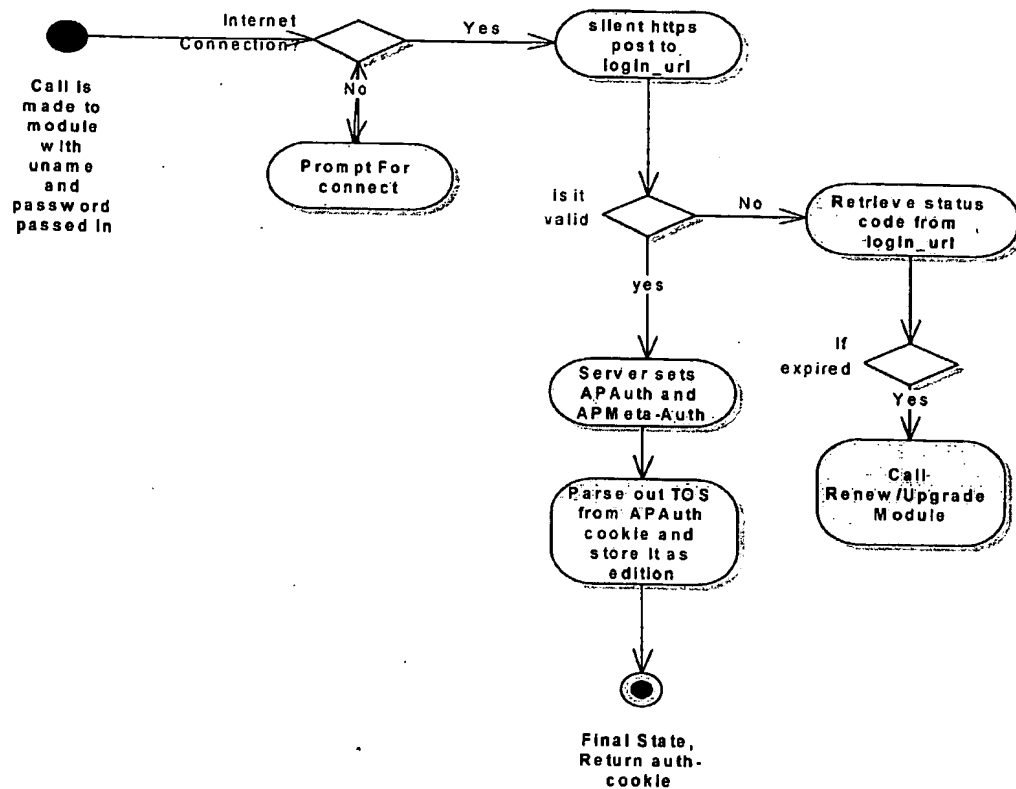
#### 9.4. Login/Authentication Module

This module will be called whenever a client process (i.e Client Proxy or the SSL server, etc... ) wants to login to the anonymizer service and receive an APAuth cookie to proceed. If auto\_login is on the calling process should pass Anon\_Uname and Anon\_Password in as the parameters. If the auto\_login is not set the calling process must prompt the user for the user name and password and then encrypt them using Anon\_Pub\_Key these will then be passed in as parameters. The module when called will do a silent HTTPS post to Login\_URL with querystring "?uname=<username> & passwd=<password>". The output of this post will be xml in this form:

```
<root>
  <status>invalid||expired||inactive||active</status>
</root>
```

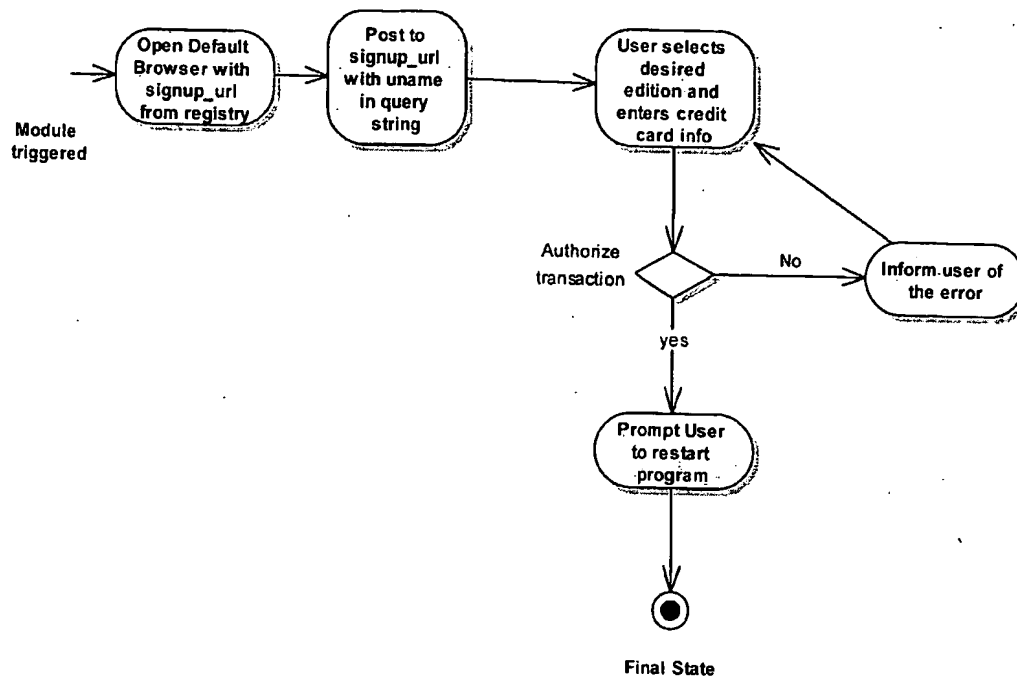
If successful APAuth and APMeta-Auth will be set and we should parse out the <tos> value from the APAuth cookie. This value will be stored in the ProductType registry entry. If not successful we will check to see if the user is expired if so call the update/renew module. If there is any other error it will be returned to the calling process, which will be responsible for re-prompting the user for his/her info.





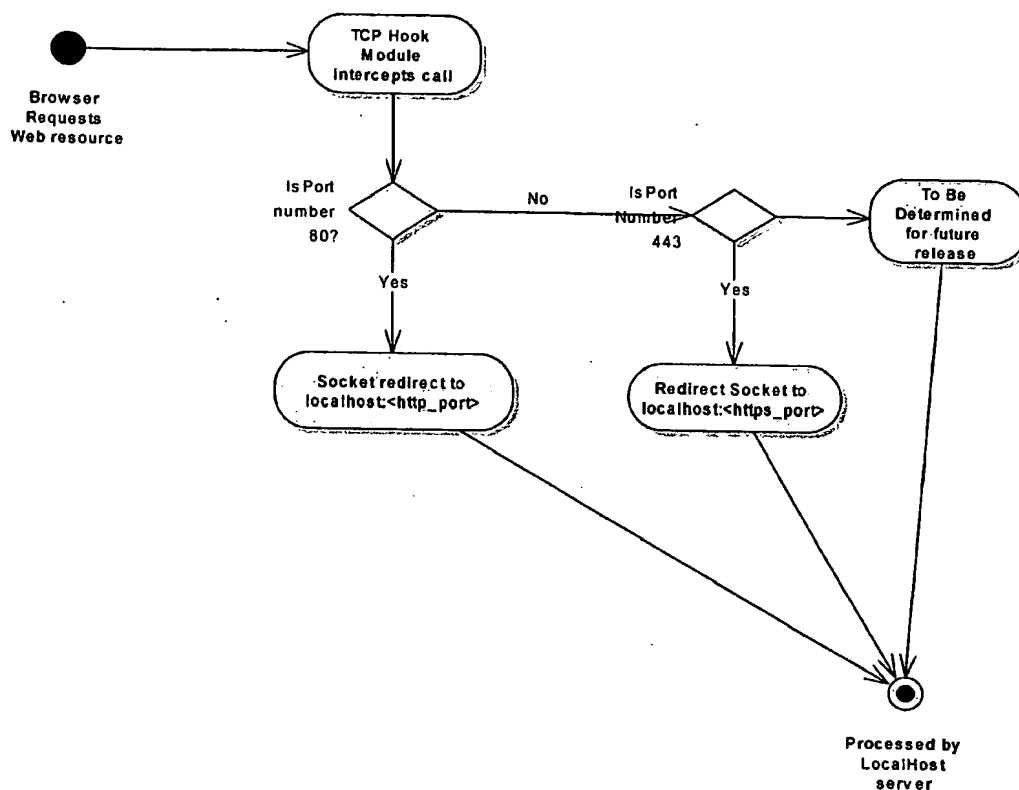
## 9.5. Renew /Upgrade Module

This module will need to be called whenever we want to prompt the user to upgrade or renew their product. When invoked it will open the default browser with the Signup URL that we have stored in the registry posting the following query string "?uname=<encrypted username>". From here the user will select the edition he/she wants to renew or upgrade and enter his/her info. Upon successful completion it will prompt the user to restart the client.



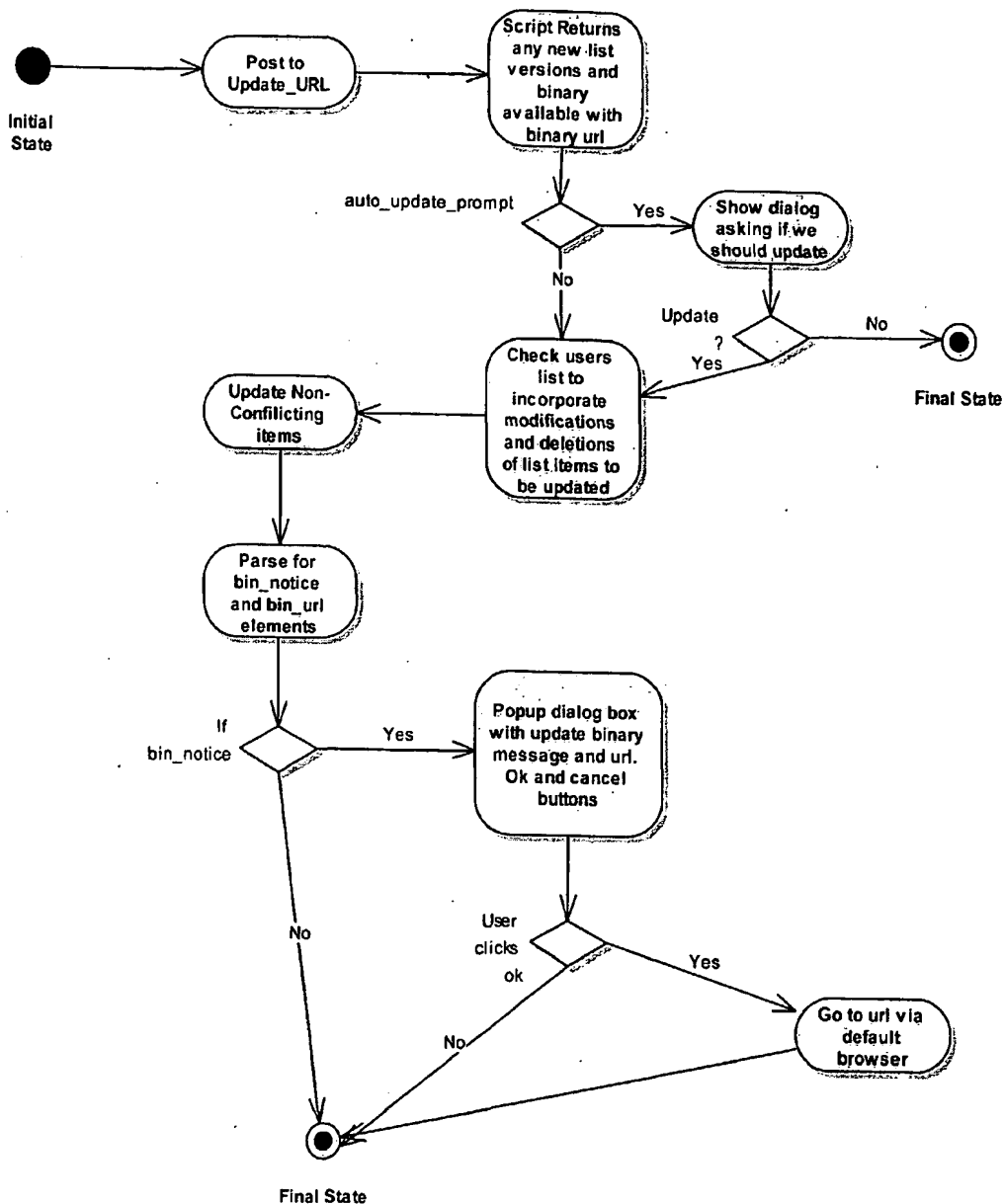
## 9.6. TCP Hook module

This module is responsible for hooking all the necessary tcp layer calls and redirecting the data to the client proxy module. When the browser tries to connect a socket the TCP Hook module will intercept the call and examine the port number. If it is 80 it will redirect the socket to localhost with the port set to the registry value (http\_port). If it is port 443 it will redirect the socket to localhost with the port set to the registry value (https\_port). If it is any other port it will redirect to localhost with port 8080.



## 9.7. Client Update Module

When the client update module is called it will make a silent http post to the Update URL. This script will return any new list versions and a bin\_notice with a bin\_url based off the information in the AnonPro cookie. If Auto update prompt is set to 1 then we must pop up a dialog to see if we should update the lists. If they answer yes we proceed if they answer no we do no update. Before writing each list into the registry we must read TrustedList, ProtectedList, BlockedList and ServerList from the registry and check for modifications or deletions by the user. If the user has done either of these then their changes should persist. If we have parsed out a bin\_notice and bin\_url then we must pop up a dialog informing the user of the binary update and asking them if they would like to download it. If they choose ok we must open the default browser and navigate to that url.

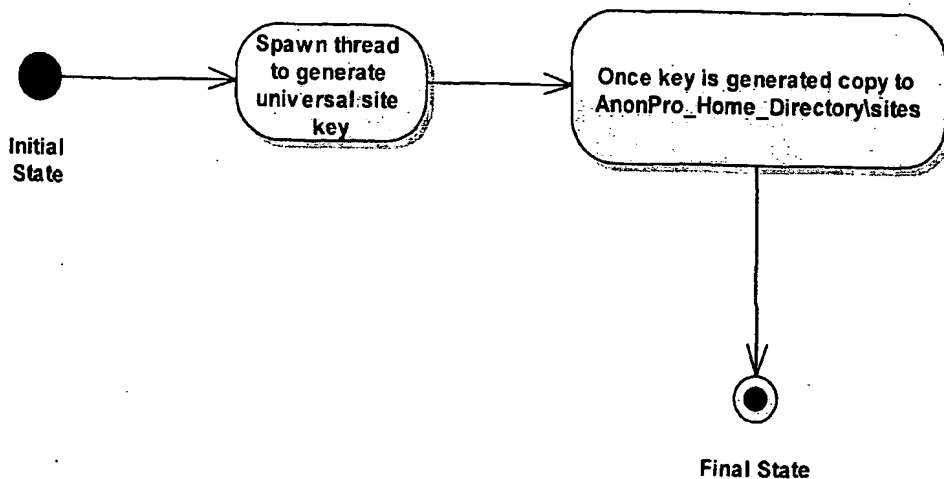


## 9.8. Client Proxy Module

This module is to be run as a windows service separate from the client. When the client proxy module starts up it must read the TrustedList, ProtectedList and the BlockedList from the registry in order to populate our per site preferences cache. This cache will be a hash table with the hash value being a hash of the top level domain and the value being the DWORD bitmask containing the preferences. These lists will be stored in xml format so they will need to be parsed.

### 9.8.1. Universal site key module

This module will be invoked once on startup to generate a new universal site key to use for the current session. This key will be used to forge the identity of all ssl servers the client tries to connect to. It will be invoked as a low priority thread to run in the background and generate the key. Once the process is finished it will swap the new key for the current one and exit. To generate this key pair we will use the OpenSSL functions to create the RSA key pair. Once generated this key pair is it will be stored encrypted using the SHA-1 hash of the username and password in AnonPro\_Home\_Directory\sites. We will also need to write a function to generate the site certificates when we need them. This will just take the domain name as a parameter that will be inserted into the cert template and then signed by the secret key generated above.



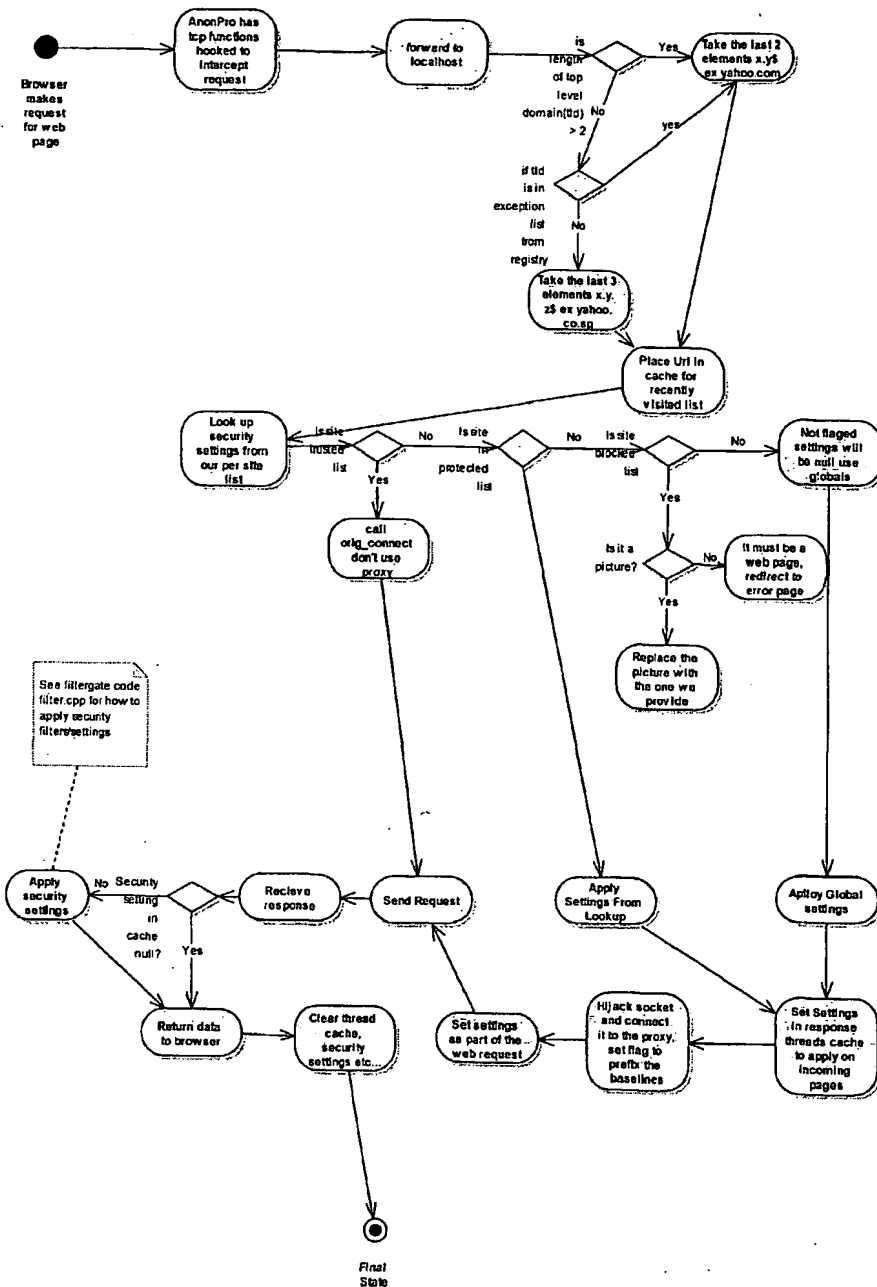
### 9.8.2. SSL module

This module is responsible for the handling of all data passed through on a secure connection. This is outside the scope of this document and will be discussed in a separate specification.

### 9.8.3. Non-SSL Module

This module is responsible for the handling of all data passed through that is not on a secure connection. Its primary responsibility will be adding and removing headers as well as streaming the data through the filter module and the anonymizer proxy. During the processing of the request this module will need to prune the url down to its top level domain and enter it into the recently visited sites cache (Recently visited sites) It will also need to run the top level domain through the per-site settings cache to see if there is a match. If there is we will apply those security settings to this request if there isn't we will use the global

settings ( Security Level ) . Once we have applied all of our security filters we will forward the request to the anonymizer proxy. When we receive the response from the anonymizer proxy we will do a second pass on our filters applying those that are relevant to incoming requests. Finally we will return the requested web resource to the browser.



#### 9.8.4. Filtering Module

This is the module responsible for filtering the content requested by the user. It will remove items such as ads, popups etc... (Refer to the requirements features matrix ). This functionality is already implemented in the filtergate code. It will either be moved to and called by the client proxy or it will be called through filtergate via the shared memory interface. One thing to note is that we will now be collecting stats on how many threats we have blocked. We will need to update the PagesBlocked, ActiveContentBlocked, AdsBlocked and PopupsBlocked to reflect what we have done. This can be updated either on a per item (meaning every time something is blocked you update the count) or on a per page basis (meaning you keep counts for every page and update the counts after the page is finished loading). If while filtering we encounter a request that is on the blocked list we must redirect to Never List Redirect URL if it is a url or redirect to Never List Redirect Image if it is a request for an image. If OS hiding is active we must replace the OS in the headers with OS Hiding Name. Similarly if referrer hiding is active we must replace the referrer header with Referring Hiding Name.

#### 9.8.5. Per Request preferences

Client has to pass the following settings to the Proxy for each web-page request.

- IP-Hiding (proxy)
- SSL Fulltime (proxy)
- Active X Filter (finjan)
- Java Filter (finjan)
- JS filter (proxy)
- VB filter (finjan)
- Safe cookies

The client is to send an HTTP header with each web request that will contain a bit-mask specifying what security options will be applied by the proxy on the returned web-page that the user has requested.

Structure:

```
To check if the nth bit is turned off,  
If (2^n & bitmask == 0)  
// this means that it is turned off  
{  
  blah blah;  
}
```

### 9.8.6. Dependency Matrix

	PB	AB	3P	WB	RH	PTH	OSH	MC	BC	AxB	JB	JSB	BTB	Bm	IPH	SSL	F
PB	O																
AB		O															
3P			O														
WB				O													
RH					O												
PTH						O											
OSH							O										
MC								O									O
BC			O						O								
AxB										O							X
JB											O						X
JSB												O					X
BTB													O				
Bm														O			
IPH															O		
SSL																O	
F								O		X	X	X			O		O

Legend of Abbreviations in above table

O = Dependent (if on option is selected, the other will have to automatically be activated as well)  
X = both cannot be selected and therefore the AnonPro Client needs to deselect the other option.

PB = PopUp Blocking  
AB = Ad Blocking  
3P = 3rd Party cookies  
WB = Web Bugs  
RH = Referrer Hiding  
PTH = Page Title Hiding  
OSH = OS Hiding  
MC = Modified Cookies (also called filter cookies)  
BC = Block Cookies  
AxB = Active X Blocking  
JB = Java Block  
JSB = Java Script Block  
BTB = Blinking Text Block  
BMB = Background Music Block  
IPH = IP Hiding  
SSL = SSL Fulltime  
F = Filtering of Java, JavaScript, VBScript and ActiveX.(\*)

Browser begins streaming

- SSL
  - o If SSL (if the connection coming in is an ssl connection>
- Redirect to proxy
  - o IP hiding
  - o URL encryption
  - o Ssl



- Rewrite headers
  - o OS hiding (already done by FilterGate)
  - o Referrer hiding (already done by FilterGate)

For example in URL encryption, the the public key is stored by anonpro client in a cookie. The proxy will then pick up this cookie. (Currently the toolbar does it this way – but not with an XML structured cookie).

**Note: Proxy Changes will be needed to support XML cookie structure.**

### **9.8.7. Preferences**

#### **Trusted List / Protected List**

- check "Blocked" list, then check "protected" list, then check "trusted" list
- if URL is listed in the "blocked" list
  - o if it is the HTML mail page – popup a warning
  - o if it is just an image, replace the image with an "anonpro" image
- If the URL is listed in the "protected" list:
  - o Check the "per site" preferences
  - o If no "per site" preferences, then use what the current preferences are.

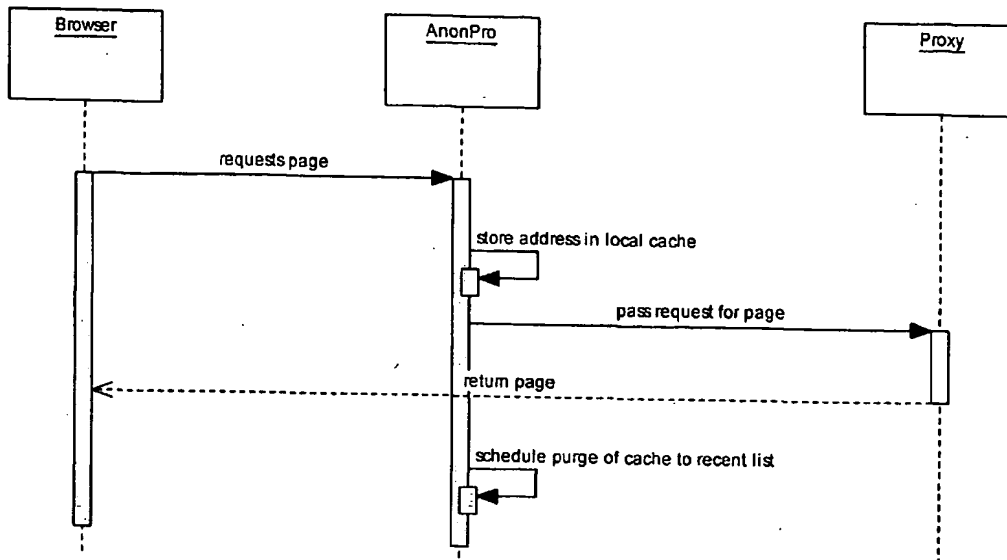
### **9.8.8. Java Script cookies**

In this release we will keep the current java script cookie functionality that resides in the proxy and leave it there. In a later release of the AnonPro Client, we will include java script cookie functionality.

### **9.8.9. Modified Cookies**

If this is on we will set all of the cookies to session only. We will override the javascript setcookie functionality to set its cookies as session only as well.

## 9.9. Recently Visited Sites



Whenever a request is made for a web page the address is placed inside our cache. At some point a thread will be scheduled to go through the cache pruning addresses down to their top level domains, removing duplicate entries and placing any new domains into the recent hash map.

Note to developer, how do you plan on pruning top level domains. You have .us.gov etc...

Whenever a request is made for a web page the address is placed inside our cache, we will need to schedule a thread that will run somewhat frequently to go through the cache using our url pruning algorithm to strip down to top level domains removing duplicate entries and placing any new domains into the recent hash map.

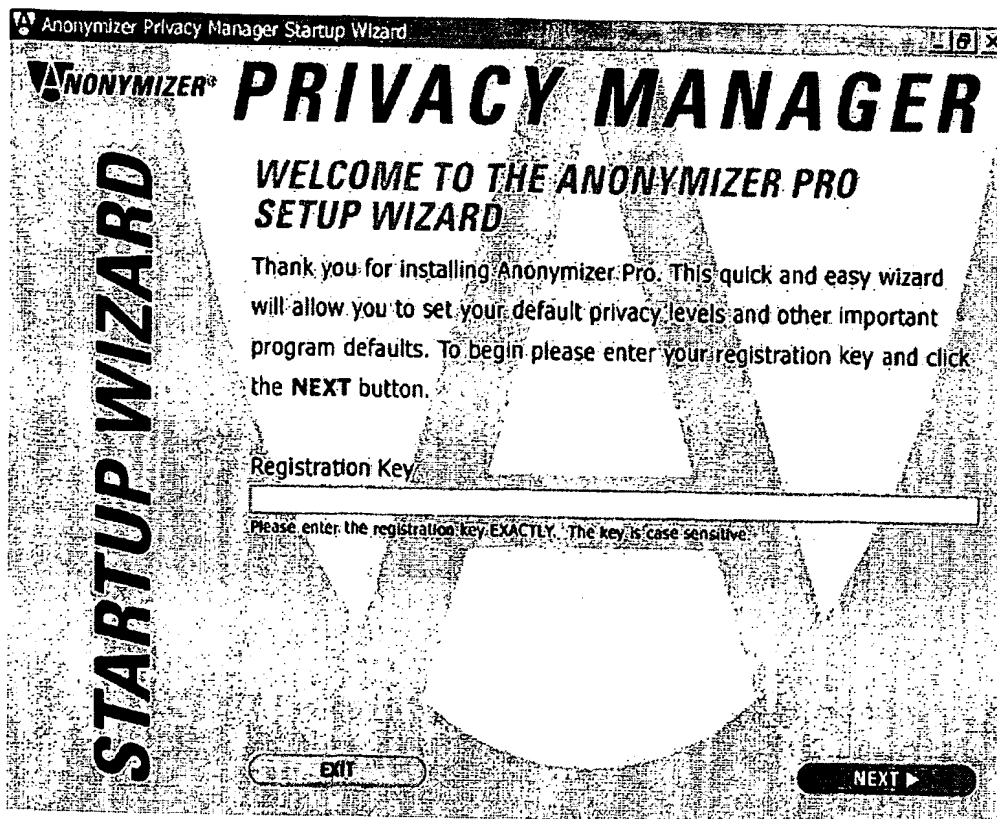
## 9.10. GUI

The aim of our user interface is to allow the user to easily navigate through the control settings for the AnonPro Client. The interface should be simple and easy to use. In addition the GUI should be able to meet the current demands and able to evolve to meet future challenges.

### 9.10.1. Start Wizard

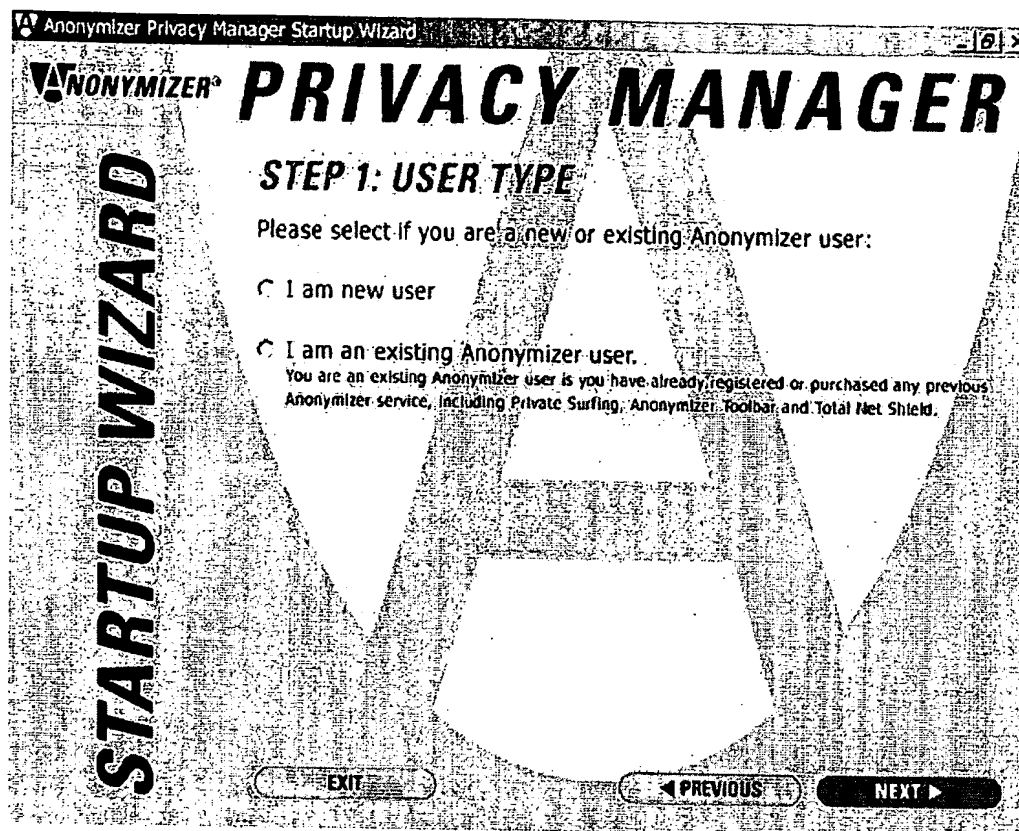
#### 9.10.1.1. Welcome

When the client is started, it is loaded into the system tray and displays as an icon. Immediately after that, the client checks to see if it is being run for the first time (*"Is initial run?"*) by reading the registry setting (*Initial Execution*). Please see section *"3.2. Startup Wizard Module"* for details of the startup wizard.



The registry setting is used to indicate if the wizard needs to run or has already run. During client installation, this needs to be set to 0 by the installer. After "startup wizard" is run, the client has to change this flag to "1".

#### 9.10.1.2. User Type setup



### 9.10.1.3. New User Registration

Anonymizer Privacy Manager Startup Wizard

**NONYMIZER®** **PRIVACY MANAGER**

**STARTUP WIZARD**

**STEP 2: NEW USER REGISTRATION**

Username

Password

Confirm Password

E-mail

Confirm E-mail

**EXIT** **PREVIOUS** **NEXT**

#### 9.10.1.4. Existing User Registration

The screenshot shows a window titled "Anonymizer Privacy Manager Startup Wizard". On the left, a vertical banner reads "STARTUP WIZARD". The main title is "PRIVACY MANAGER". Below it, the step is "STEP 2: EXISTING USER REGISTRATION". There are two input fields: "Username" and "Password". At the bottom, there are three buttons: "EXIT", "PREVIOUS", and "NEXT". The "NEXT" button is highlighted.

Anonymizer Privacy Manager Startup Wizard

**PRIVACY MANAGER**

**STARTUP WIZARD**

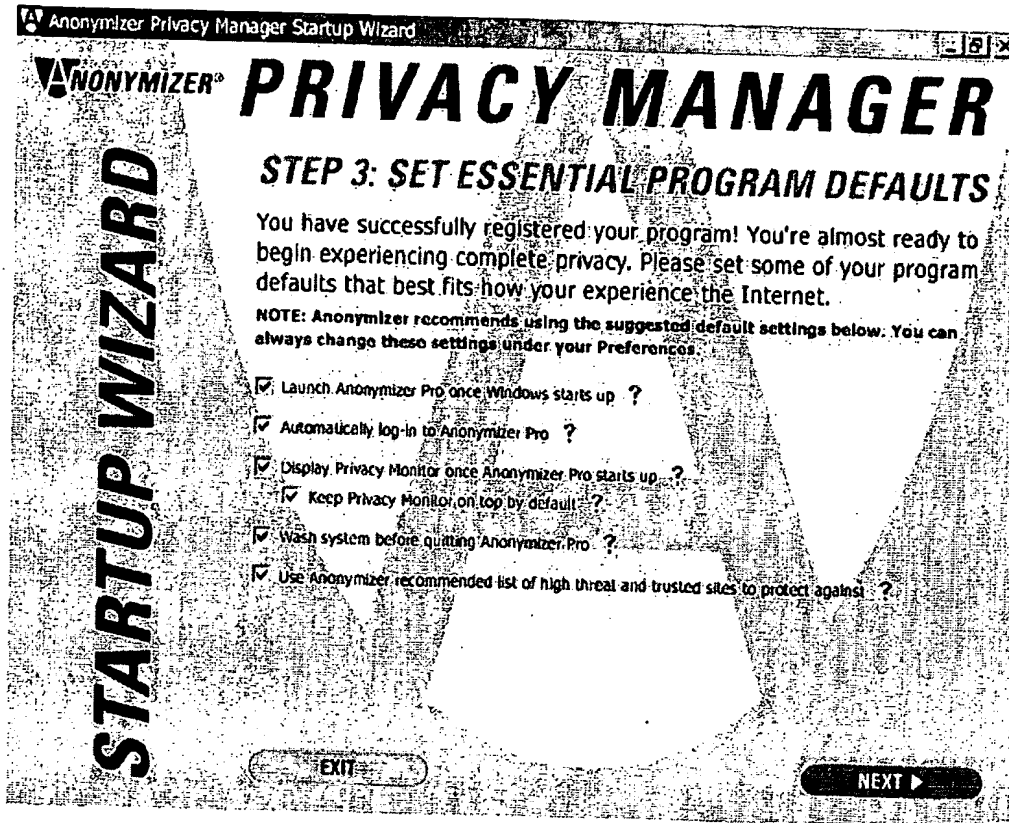
**STEP 2: EXISTING USER REGISTRATION**

Username

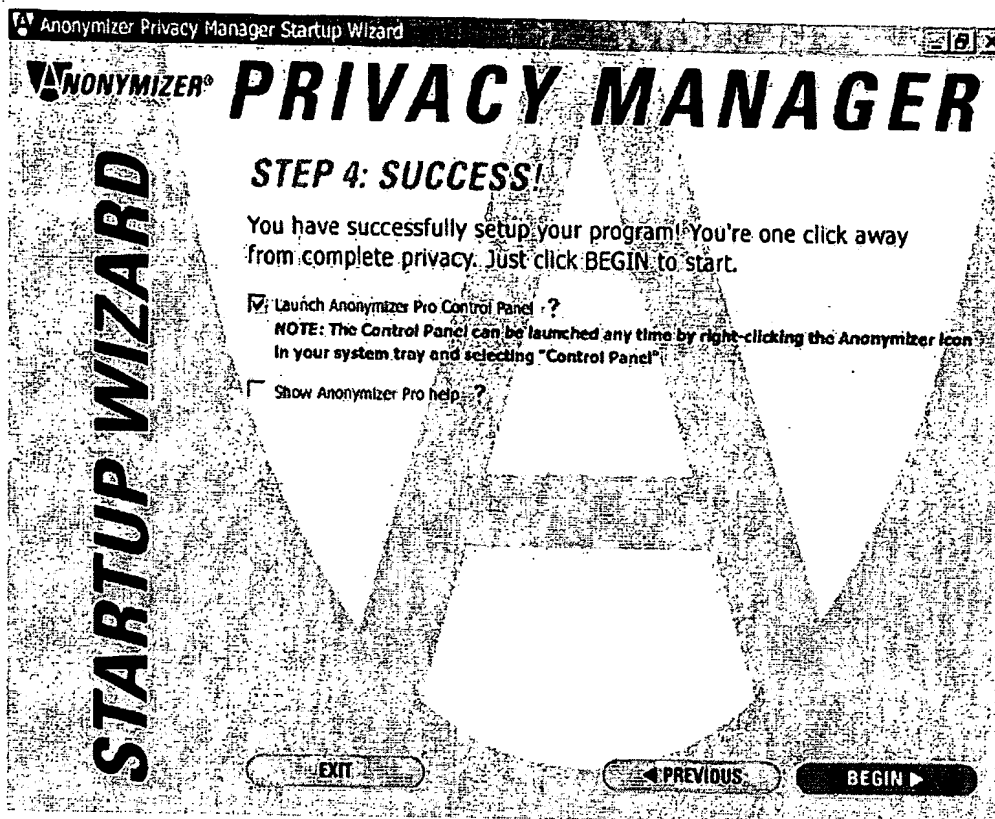
Password

EXIT PREVIOUS NEXT

#### 9.10.1.5. Set Essential Program Defaults



#### 9.10.1.6. Success



#### 9.10.2. System Tray

The AnonPro client installs into the system tray within windows. The Sys.Tray Icon is that of the Anonymizer logo (a blue shield with an "A" in the middle). By hovering over the blue shield with the mouse and right or left-mouse-click, a menu will display.

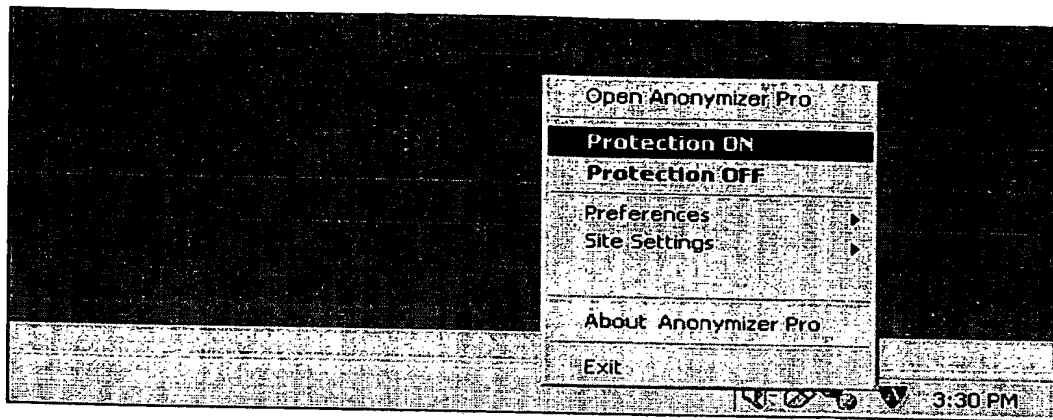
The menu contains the following items:

- Open Control Panel
- On/Off toggle
- Per Site-Settings
- About AnonPro
- Exit

Below is an example of the system tray with opened menu list. The menu items in the example below are different than the actual requirements as listed above. The menu items from the list above are accurate and override those shown in the screenshot below.

Right mouse pulls up menu. Left mouse pulls up control panel.






#### 9.10.2.1. Default Screen


The first screen that is display when the user clicks on the AnonPro icon in the sys tray or selects "Open Anonymizer Pro" is the "Global Settings" screen.


#### 9.10.3. Bitmap images


Below are a list of the various images that are needed for the GUI.

In order to be consistant with our Control panel button colors, we have the icons change colors depending on state of application:

ON = Green Anonymizer Icon  (this icon shows blue – but change this to green)

Off = Red Anonymizer Icon 

32x32 Icon = 

16x16 image for trash = 

Slider Background =

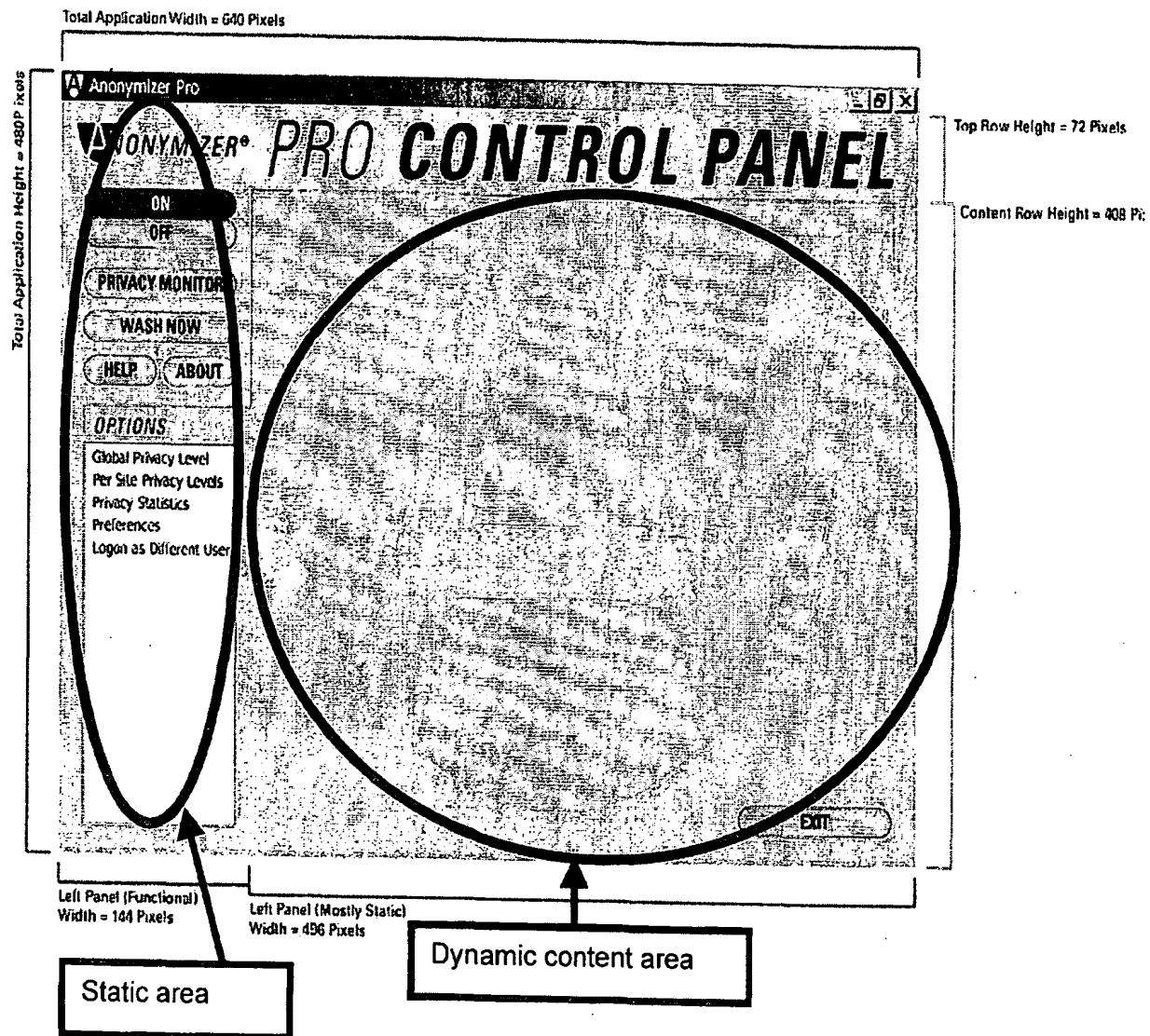


#### **9.10.4. Non-Categorized Screens**

1. All miscellaneous pop-up boxes (such as "enter user-id and password" popup) will carry over the same look and feels as that of the of the control panels (buttons, colors, text).

### 9.10.5. Static Areas of Control Panel

The control panel is split up into 2 "frames". The frame on the left is a "static area" which does not change between the various screens of the control panel. The frame on the right is the dynamic area of the control panel and will show different values and functionality for each screen.



#### 9.10.5.1. Static Button attributes

"On" button – if selected – turns green. If not selected – turns gray. If mouse hover – text in button turns yellow. If pressed down, the button will turn a darker color of the color it currently is (e.g. green – turns dark green, gray – turns dark gray). Please see [Appendix C: Color RGB matrix](#) for the RGB values of the listed colors.

**"Off" button** – if selected – turns red. If not selected – turns gray. If mouse hover – text in button turns yellow. If pressed down, the button will turn a darker color of the color it currently is (e.g. green – turns dark red, gray – turns dark gray). Please see ["Appendix C: Color RGB matrix"](#) for the RGB values of the listed colors.

**Privacy Monitor** – if selected – turns green and brings the privacy monitor to the front (if the privacy monitor is already activated, then it is brought to front). If not selected – turns gray. If mouse hover – text turns yellow. If pressed down, the button will turn a darker color of the color it currently is (e.g. green – turns dark green, gray – turns dark gray). Please see ["Appendix C: Color RGB matrix"](#) for the RGB values of the listed colors.

By selecting the privacy monitor – a small window displays (separate to the control panel), at the bottom-right corner of Windows, statistics on the privacy functions that are working (as selected by the user in the "privacy settings" control panel). For example the "privacy monitor" would display the privacy values for a given page with count statistics.

If the "docking" option in preferences screen (see ["Preferences"](#) section) is selected, then the "privacy monitor" screen is placed at the bottom right corner of the windows desktop.

Note the picture of the "privacy monitor" below shows a window pane with a title frame. The final "privacy monitor" should not have a title frame, but should just have a thin frame. If the use wants to move the window, then he/she can click anywhere on the window and drag it with the mouse. Also, there is no min/max or close buttons as shown in the example below since this is a title-less window.

#### **Paid Privacy Monitor**

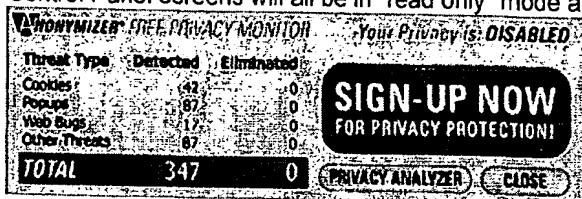
The privacy monitor GUI has been modified to a much simpler design. Please see below for the new GUI design.



#### **Free Privacy Monitor**

Also, one edition is possible. This is if the user buys the "Privacy Monitor Only" edition (which will likely be a "freeware" product). Its purpose is to scare the user into seeing how much is actually being sent to their computer that might breach their confidentiality.

The AnonPro client will not actually filter or block anything (e.g. all functionality is turned off). The Control Panel screens will all be in "read only" mode and all GUI checkboxes will be inactivated.



**Wash Now** – if selected – turns green for 5 seconds (to simulate washing). If not selected – turns gray. If mouse hover – text turns yellow. If pressed down, the button will turn a darker color of the color it currently is (e.g. green – turns dark green, gray – turns dark gray). Please see ["Appendix C: Color RGB matrix"](#) for the RGB values of the listed colors.

The wash now button will call the AnonWasher application (not part of the AnonPro Client and sold separately). The AnonPro Client will know where the executable of the AnonWasher by reading the registry setting: "AnonWasher\_Home".

**Help** – if selected – turns green and pops up a separate "Help" window (see section 4.4.7. below). If not selected – turns light gray (as shown above). If pressed down, the button will turn a darker color of the color it currently is (e.g. green – turns dark green, gray – turns gray). If mouse hover – text turns yellow. Please see "Appendix C: Color RGB matrix" for the RGB values of the listed colors.

**About** – if selected – turns green and pops up a separate "About" window (see section 4.4.8. below). If not selected – turns light gray (as shown above). If mouse hover – text turns yellow. If pressed down, the button will turn a darker color of the color it currently is (e.g. green – turns dark green, gray – turns gray). Please see "Appendix C: Color RGB matrix" for the RGB values of the listed colors.

**Options** – There are 4 items in the options section in a list box and are detailed in the following pages:

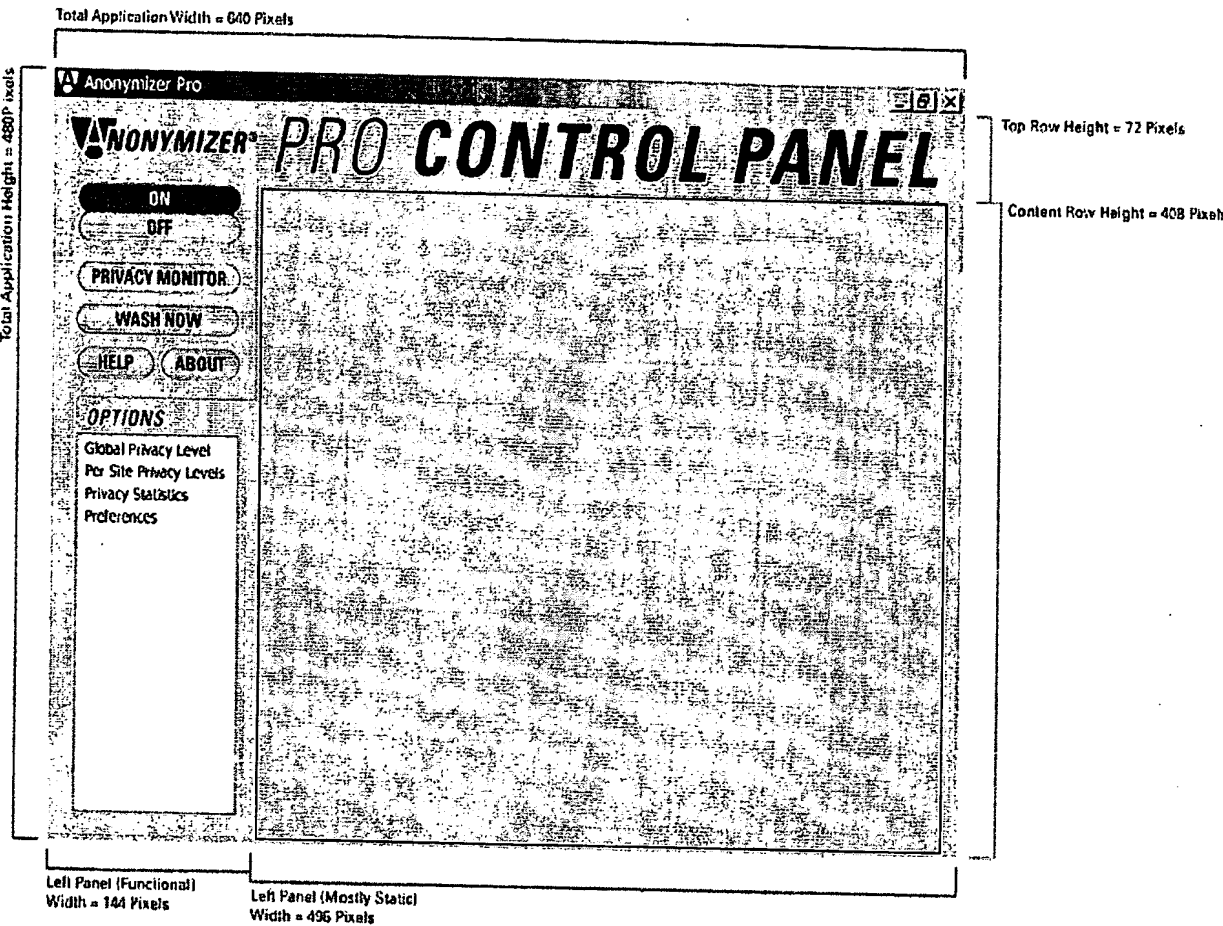
- global privacy level
- per site privacy level
- privacy statistics
- preferences

Upon selecting any of these items, the selected list item turns gray with white text.

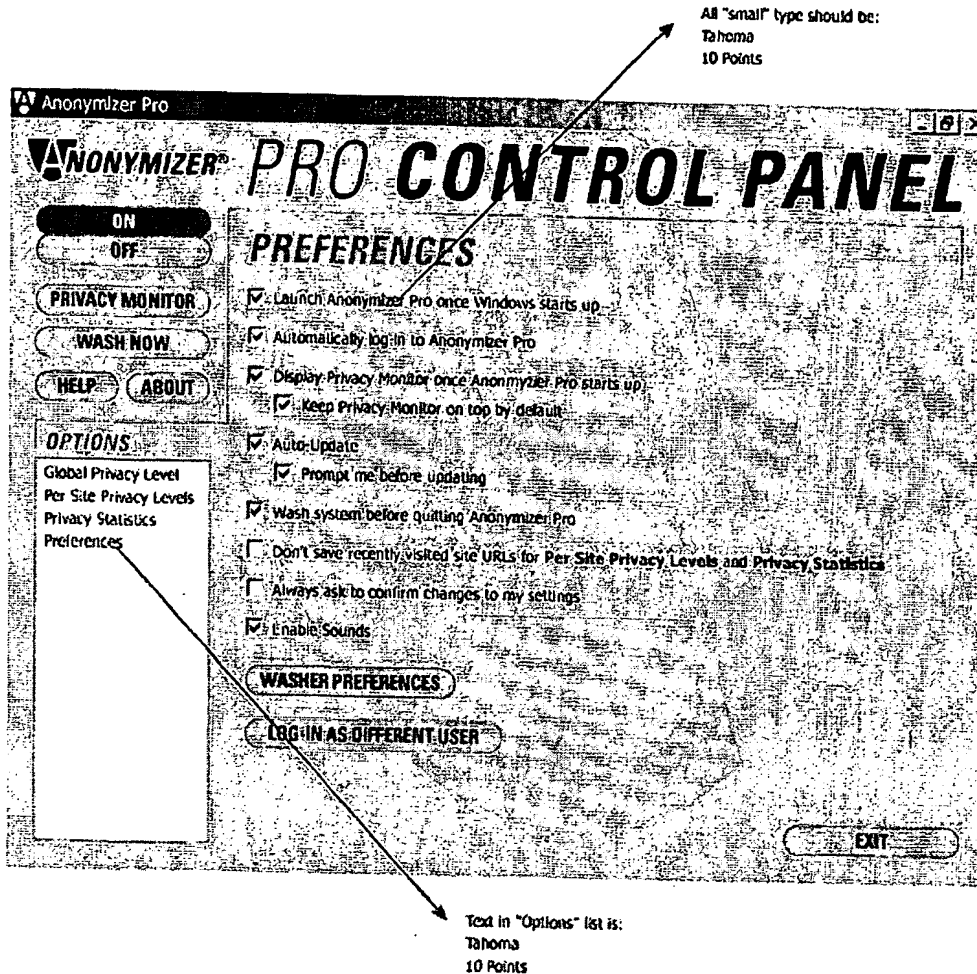
**Dialog Size** – All control panel window sizes are fixed (and not sizable). The Size of the control panel should be determined upon creating the actual GUI to ensure that no restrictions on displaying all functionality caused in displaying the control panel window.

**Minimize/Max** – Pressing the minimize puts the window in the task bar of windows. Prefixing "X" closes the window and hides the control panel in the system tray. Maximize does nothing – as the window is not sizable.

9.10.6. Dimensions



### 9.10.7. Preferences



Please note: The diagram above shows the Logon as different user as a menu item. But actually this should be a box in the "Preferences" section. It is not logically possible to be able to switch user's AnonPro settings from this screen and therefore might confuse the users. Rather "Logon" as different user should be to allow the user to logon using a different user-id/pw to logon to the Anonymizer web-site. If the user wants to load different AnonPro Client settings, then he/she will need to logout of windows and relogin as a different user. The HK\_Current\_User registry handles this in the matter consistent with typical windows applications.

#### 9.10.7.1. Launch AnonPro once windows starts.

In the preferences settings GUI, the user has the capability of specifying whether the AnonPro client should start automatically when windows start – or not. If the user selects this option, the registry setting "<HKCU> Run\_when\_win\_starts" will be set to "1" (on). Upon AnonPro client startup, it will read this registry setting to determine if anonpro should be started and will do so accordingly.

#### **9.10.7.2. Automatically log-in to AnonPro**

In the preferences settings GUI, the user can select whether AnonPro logs the user in and authenticates the user with the Anonymizer Web-Server. If "remember me" is selected by the user, the AnonPro client will read this setting from the registry (<HKCU> Auto\_login) upon startup and automatically log the user in using the registry values stored in (<HKCU> Anon\_Uname and <HKCU> Anon\_Password) and logon to the Anonymizer Web-Site using these values in order to authenticate the user with the anonymizer. If the user has selected "remember me" but did not supply (and store) a user-name and password, a dialog box will appear which prompts the user to enter their user-name and password (with the option to store these values permanently). In which the preferences screen above should also have a button to the right of this option "user-name and password" that allows the user to pull up the same dialog box. But this is not shown in the screenshot above. This needs to be added to the screenshot and included in the next version of this document.

#### **9.10.7.3. Display Privacy Monitor once AnonPro starts up**

In the preferences settings GUI, the user can select whether AnonPro Privacy monitor automatically is displayed once the client starts up.  
In addition, the user can indicate if the privacy monitor always be on top or not.

#### **9.10.7.4. Auto-Update**

In the preferences settings GUI, the user can select whether he/she will be notified of an auto-update of lists and binaries. During Authorization, the Web-Server will check to see if any new files are available for uploading to the client. If so, these files will be uploaded to the client.

NOTE: This only happens if the user has selected this option as ON.

Registry entry: <HKCU> Auto\_Update

#### **9.10.7.5. Prompt me before updating**

In the preferences settings GUI, the user can select whether he/she will be prompted each time for new lists before they are automatically inserted. If this option is checked, each time

Registry entry: <HKCU> Auto\_Update\_Prompt

#### **9.10.7.6. Wash System before quitting AnonPro**

In the preferences settings GUI, the user has the capability to specify whether the AnonWasher should "wash" when the client is quit. Important note: If the client is turned off – then the wash is not performed. It is only if the client is quit. IMPORTANT: check if the client can catch a signal from windows when it is shutting down. Registry Entry: <HKCU> Wash\_on\_pro\_quit

#### **9.10.7.7. Don't save recently saved site URL's**

In the preferences settings GUI, the user has the capability to specify whether the resently visite URL's are actually shown in the list box in the GUI "Per Site Preference Settings" (see section 3.10.7). If the user selects to turn this off, then the recently visited sites are not stored in the list box and this list box is left empty and never logs any recently visited sites.



#### **9.10.7.8. Always ask to confirm changes to settings**

Everytime they leave a screen or leave the program and have made changes, a dialog box pops up asking if they want to save changes.

#### **9.10.7.9. Enable sounds**

If selected, the sounds AnonPro sound effects are turned on. If selected, each time a cookie, pop-up, etc is filtered or blocked, a sound effect is played. (sound effect to be determined for each type of block or filter).

#### **9.10.7.10. Washer Preferences**

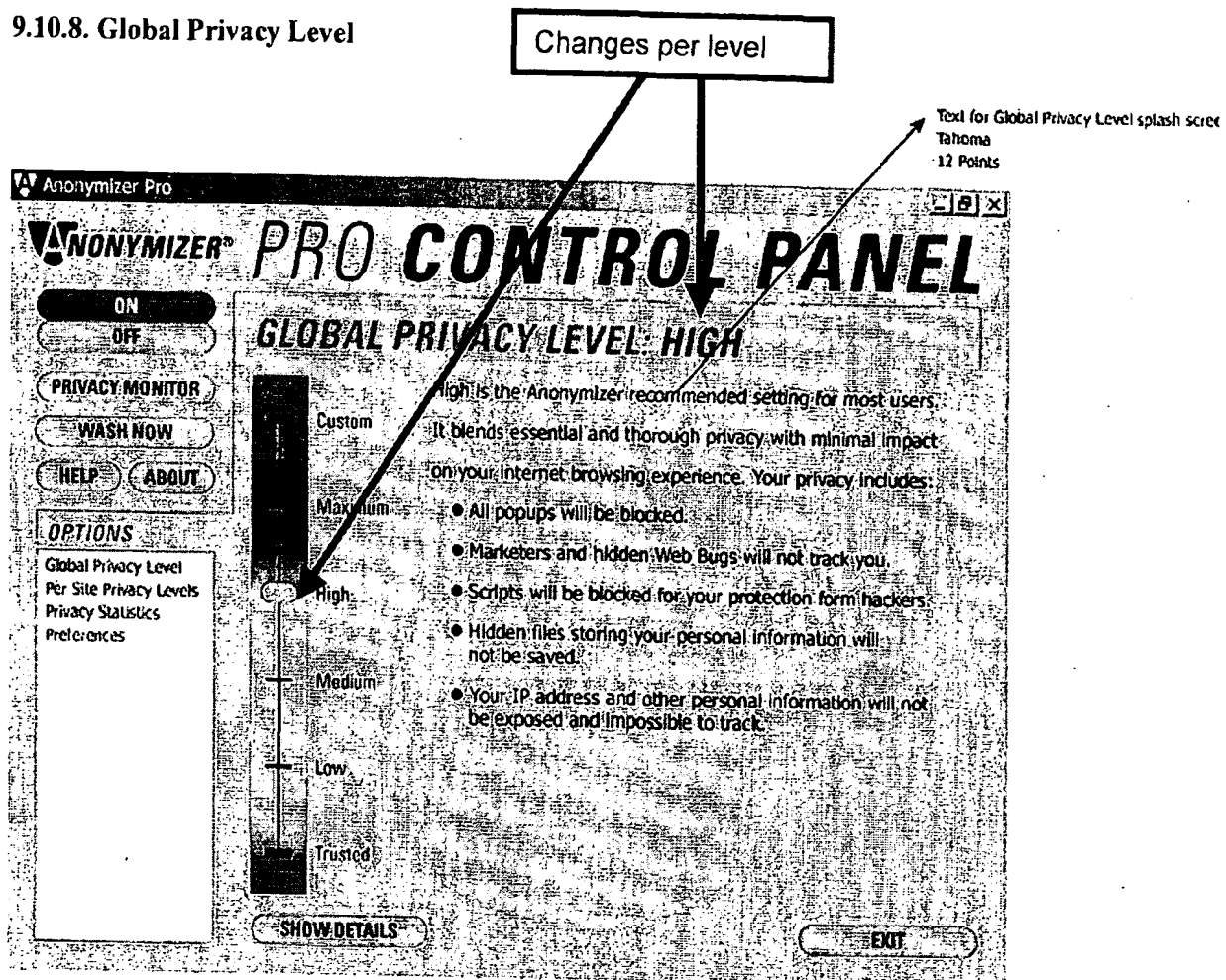
This button will pull up the AnonWasher configuration screen. AnonPro will check the registry setting of "AnonWasher\_Home" and then call the AnonWasher from the directory which is stored in this setting.

If selected – turns green and pops up a separate "AnonWasher Preferences" window (the AnonWasher is a separate application that the client calls using the AnonWasher\_Home registry setting to determine where to find the AnonWasher application). If not selected – turns gray (as shown above). If mouse hover – text turns yellow. If pressed down, the button will turn a darker color of the color it currently is (e.g. green – turns dark green, gray – turns dark gray).

Side Note: This AnonWasher\_Home registry key has to be set by the AnonWasher installer. If not, then the AnonPro Installer will set this key instead. If the AnonWasher is already installed when the AnonPro Client is getting installed, then the AnonPro Client is NOT to override this value. This is the location of the anonwasher which the "config washer" button points to and the "wash now" button points to.

There is no option in the GUI to allow where the washer resides. By default, the Washer will reside in "c:\program files\anonymizer\anonwasher".

### 9.10.8. Global Privacy Level



Please note: the threat-slider above doesn't show "blocked" – but should. If "blocked" is selected as the global setting then all sites are blocked except for those that are in the per-site settings.

#### 9.10.8.1. Slider

The slider in the global privacy level allows the user to easily change from the following levels:

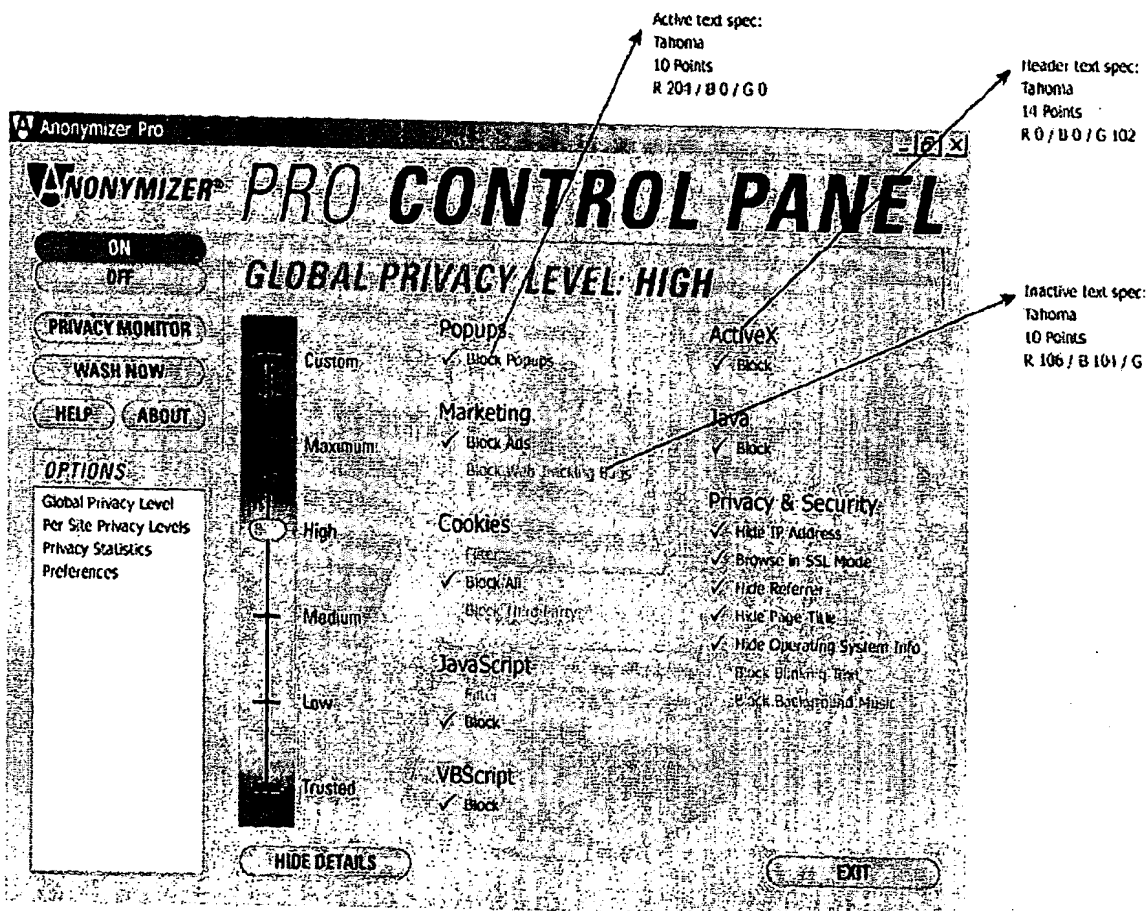
- **Trusted** - (the User selected URL does not require to go through our proxy)
- **Low** - (Protected Mode: goes through our proxy and a minimum amount of settings)
- **Medium** - (Protected Mode: goes through our proxy and a moderate amount of settings)
- **High** - (Protected Mode: goes through our proxy and a high amount of settings)
- **Maximum** - (Protected Mode: goes through our proxy and ALL settings)
- **Custom** - (Custom: gives the user the capability to select their own specific settings)

Each of the above slider settings will correspond to a pre-defined set of privacy settings. These settings as shown below as follows (needed):

### 9.10.8.2. Show Details

This will hide the explanation text and image area and replace this with details of the settings and checkboxes for each setting to turn on or off. Please see image below.

If selected – turns dark gray and replace the details to the right with an image. The button then changes text to "Show details". If "show details" is selected – turns light gray and replaces the image to the right with the details for that screen. If mouse hover – text turns yellow. If pressed down, the button will turn a darker color of the color it currently is (e.g. gray – turns dark gray).



### 9.10.8.3. Hide Details

This will hide the check boxes with the details of the settings and replace this area with an image. As of this current version of this document, we did not have the images ready. The size of the screen stays the same.

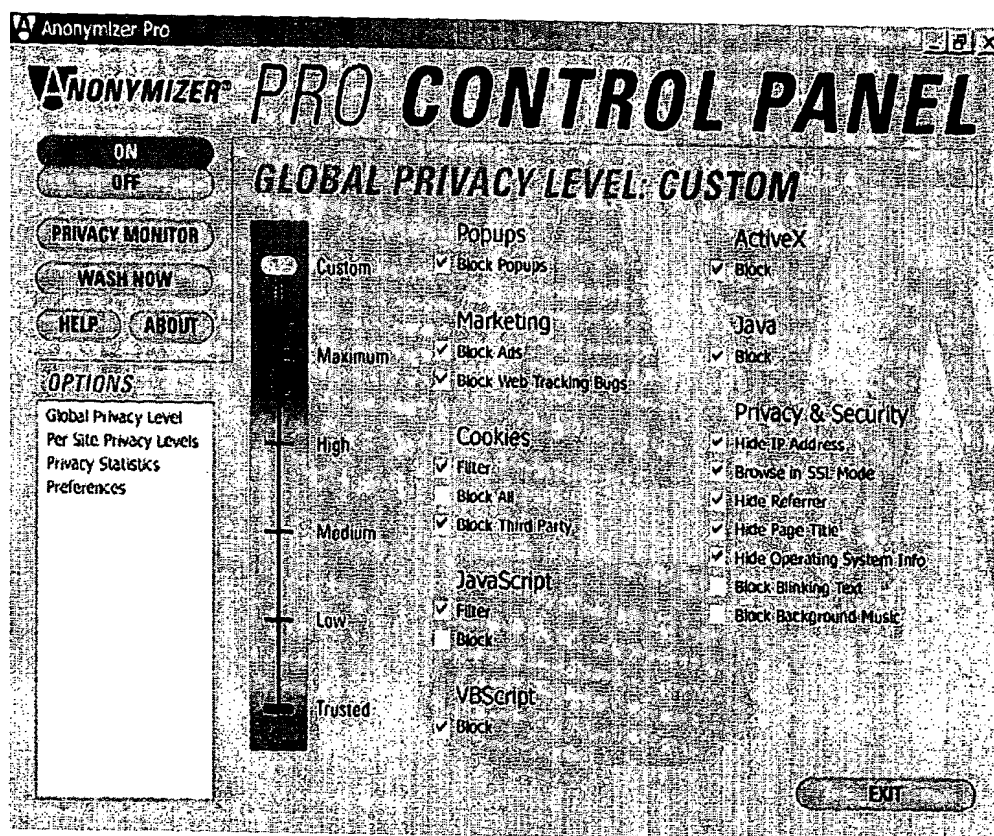
If selected – turns dark gray and replace the details to the right with an image. The button then

changes text to "Show details". If "show details" is selected – turns light gray and replaces the image to the right with the details for that screen. If mouse hover – text turns yellow. If pressed down, the button will turn a darker color of the color it currently is (e.g. gray – turns dark gray).

#### 9.10.8.4. Custom Settings

If the user moves the slider up to the "custom" area at the top of the slider, the custom settings for all functionality will be displayed with checkboxes to allow the user to either activate or deactivate each setting. The image below demonstrates how this screen will look.

Once the user changes any of the settings, these settings will be stored in the registry permanently. There is no need (or capability) for the user to save these custom settings.



#### 9.10.8.5. Matrix of different settings

Requirements features	Where	Trusted	Protected "low"	Protected "medium"	Protected "high"	Protected "maximum"	Custom
Popup Blocking	Client		X	X	X	X	Optional
Ad Blocking	Client		X	X	X	X	Optional
3rd Party Cookies	Client		X	X	X	X	Optional
Web Bugs	Client		X	X	X	X	Optional
IP Hiding	Proxy			X	X	X	Optional
Referer Hiding	Client			X	X	X	Optional
Page Title hiding	Client			X	X	X	Optional
Modify Cookies	Proxy			X	X	X	Optional
OS Hiding	Client				X	X	Optional
SSL fulltime	Proxy				X	X	Optional
JavaScript Filtering	Proxy				X	X	Optional
Active X Filtering	Proxy				X	X	Optional
Java Filtering	Proxy				X	X	Optional
VB Script Filtering	Proxy				X	X	Optional
Active X Blocking	Client					X	Optional
Block Cookies	Client					X	Optional
Java Blocking	Client					X	Optional
Java Script Blocking	Client					X	Optional
Blinking Text Block	Client						Optional
Background Music	Client						Optional

#### 9.10.8.6. Privacy and Security

##### 9.10.8.6.1. Referrer Hiding

Will suppress the referrer information that is passed in HTTP protocol. If this option is selected, the registry value: "Referrer\_Hiding\_Name" will be replaced for the tag. This value will be set during installation of the AnonPro Client and will not appear in the GUI. Therefore the use doesn't have the capability.

##### 9.10.8.6.2. OS Hiding

In the registry, the tag: OS\_Hiding\_URL - is the name that is replaced when the OS\_Hiding option is turned on

### 9.10.9. Per Site Levels

**Anonymizer Pro CONTROL PANEL**

**PER SITE PRIVACY LEVELS**

**RECENT SITES**

- yahoo.com
- hotmail.com
- msn.com
- google.com
- usc.edu
- honda.co.jp

**MY SITES**

Site	Privacy Level	Action
yahoo.com	High	EDIT
hotmail.com	Trusted	EDIT
msn.com	Medium	EDIT
google.com	Custom	EDIT
usc.edu	Low	EDIT
hacker.co.jp	Maximum	EDIT
sex.com	Block	EDIT

**Options:**

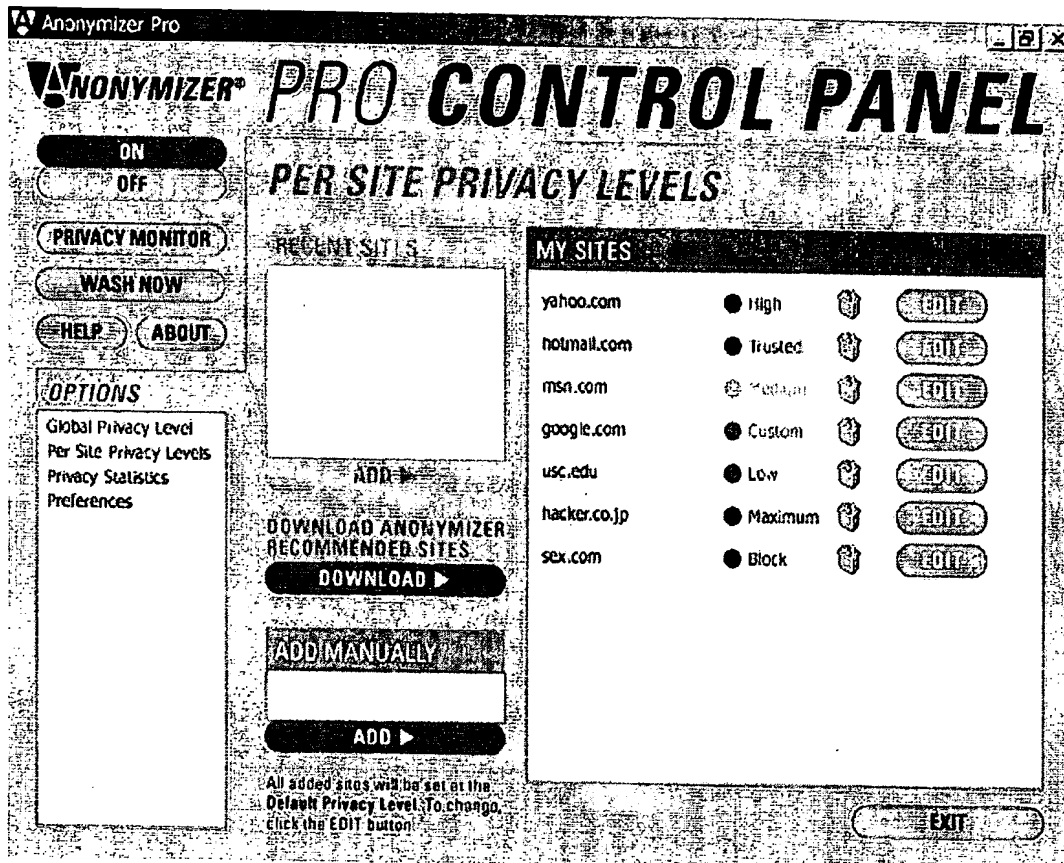
- Global Privacy Level
- Per Site Privacy Levels
- Privacy Statistics
- Preferences

**Annotations:**

- High/Maximum text spec:  
Tahoma  
10 Points  
R 201 / B 0 / G 0
- Trusted/Low text sp:  
Tahoma  
10 Points  
R 0 / B 0 / G 102
- Medium text spec:  
Tahoma  
10 Points  
R 255 / B 204 / G 0
- Custom text spec:  
Tahoma  
10 Points  
R 51 / B 102 / G 153

**Footer:** All added sites will be set at the Default Privacy Level. To change, click the EDIT button.

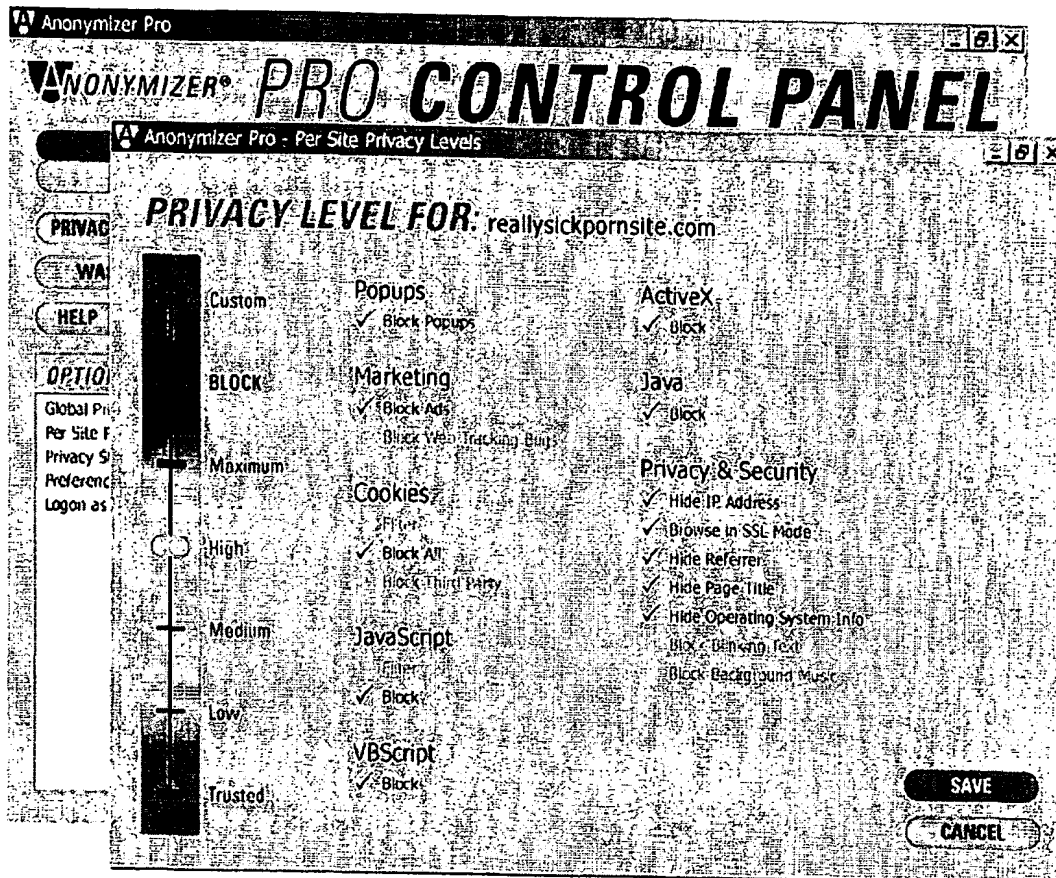
If the recent sites box is empty, and the user tries to “Add” , then the nothing happens. No error box is displayed – but rather we feel it is intuitive that the user realizes that nothing happened because there was nothing that could be selected to be added. No pop-up error is displayed.



For “Add Manually” this is the same case as well. If the user clicks on “Add” but hasn’t typed anything in the text-box, then nothing will happen. We assume that the user will realize that they haven’t typed anything in to add. No pop-up error is displayed.

If the user try to add a site that already exists in my-sites, then it acts like it adds it, but doesn’t actually because that site already exists. No pop-up error is displayed.

## Per Site Settings



If the user selects from the Threat-Bar the "Custom" level, the "non-selectable" settings are changed to "check-box" settings to allow the user to make modifications to the settings.

If the user selects from the Threat-bar the "Block" level, then the "dynamic data" section of the screen (the right hand side) does not display the actual settings (as shown above), but rather shows a summary what "blocked" means (corresponds to the "Hide settings" screens).



## Statistics

Statistics

Anonymizer Pro

# ANONYMIZER PRO CONTROL PANEL

ON  
OFF

PRIVACY MONITOR

WASH NOW

HELP ABOUT

OPTIONS

- Global Privacy Level
- Per Site Privacy Levels
- Privacy Statistics
- Preferences

## PRIVACY STATISTICS

### RECENT SITES

Site	Threat Factor	Popups	Cookies	Scripts	Privacy Level
yahoo.com	● High	17	23	247	SET
msn.com	○ Medium	24	8	123	SET
hotmail.com	● Low	3	17	182	SET

### MY SITES

Site	Threat Factor	Popups	Cookies	Scripts	Privacy Level Set
yahoo.com	● High	17	23	247	● High
hotmail.com	● High	17	23	247	● Trusted
msn.com	● High	17	23	247	○ Medium
google.com	● Low	17	23	247	● Custom
usc.edu	○ Medium	17	23	247	● Low

EXIT

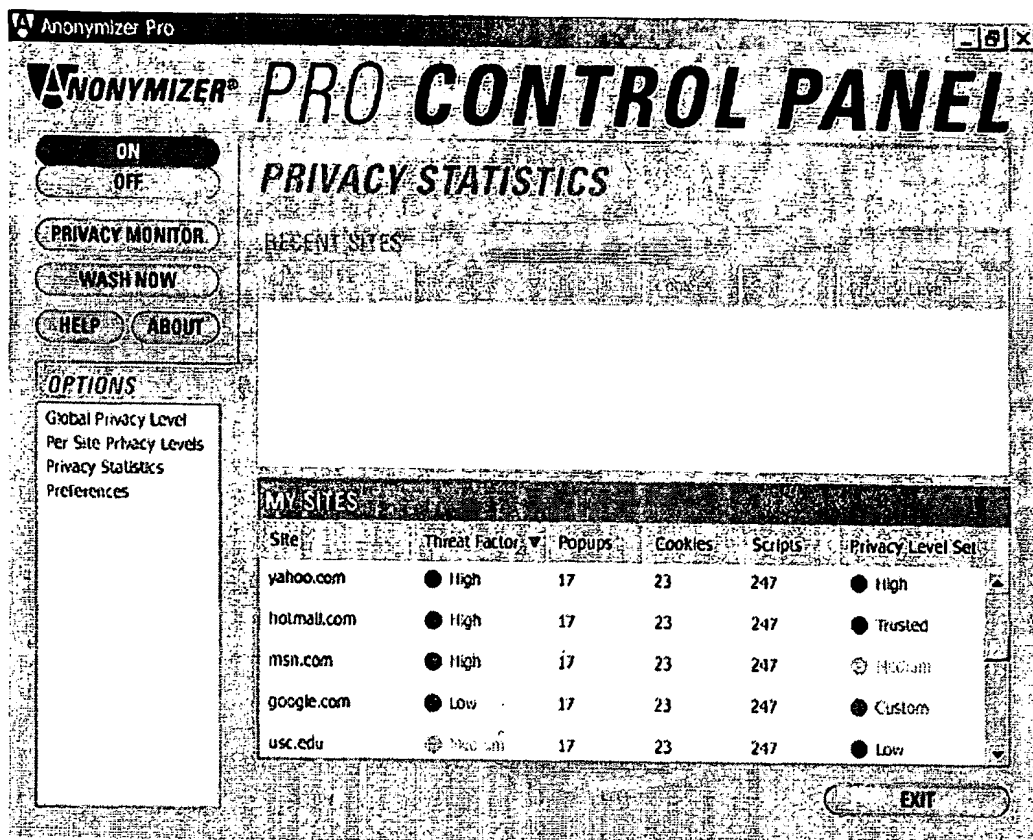
From the screen example above, the arrow indicates, sortable. There are 2 columns that are sortable - "site" and "Threat factor". All other are not sortable.

If the user decides to "set" a sites privacy settings from the "recent sites" list, then site is moved to the My Sites section of the screen after the user has finished setting.

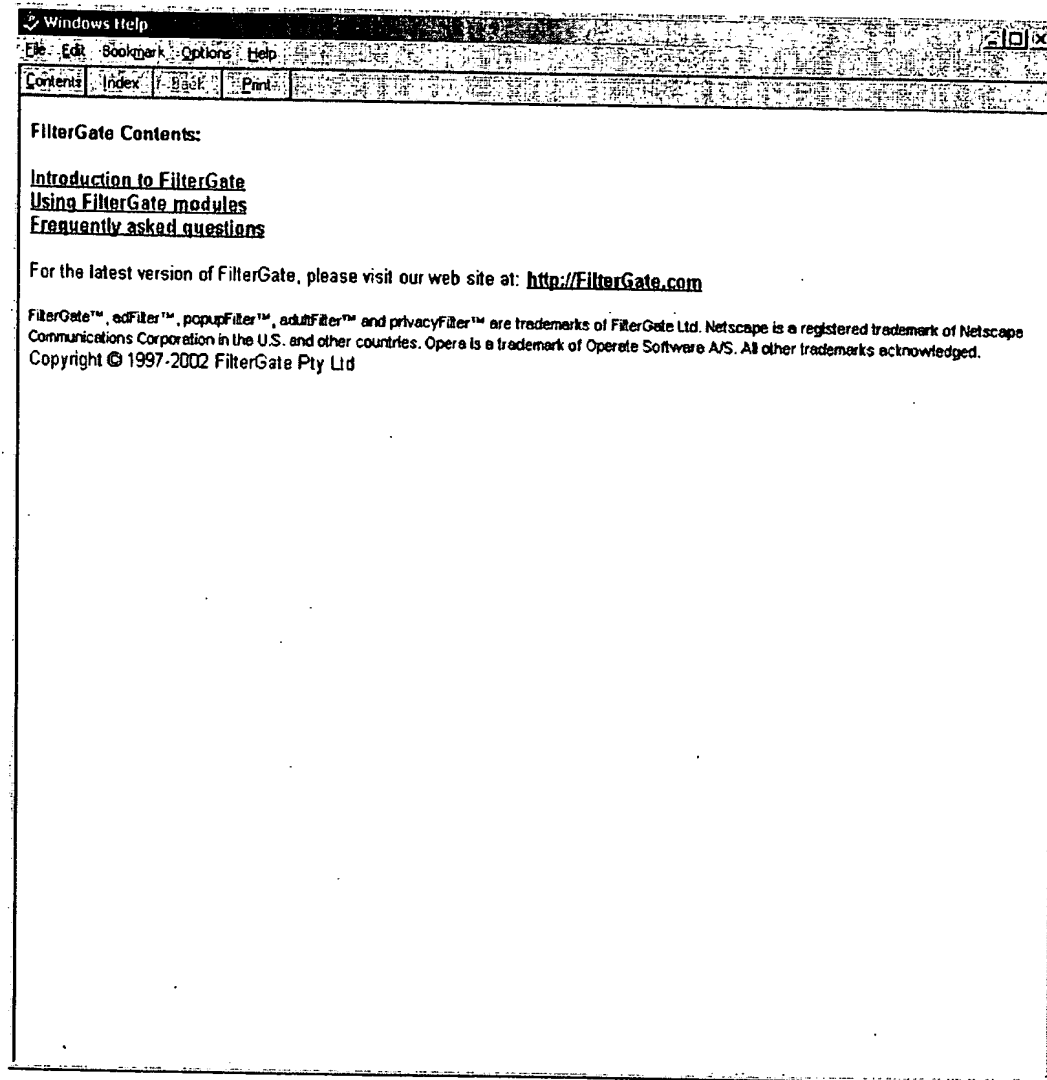
The my sites needs to be able to allow them to be "set" as well. Therefore, in the "my sites" section we will have a gray button background behind the actual current level setting. If the user selects, then it allows for editing of the per-site settings and pop up the per-site perf. screen.

Please note: Still needs is a definition of what the derived 'threat factor' for any site.

E.g.: High, medium or low. We need a matrix to map out.

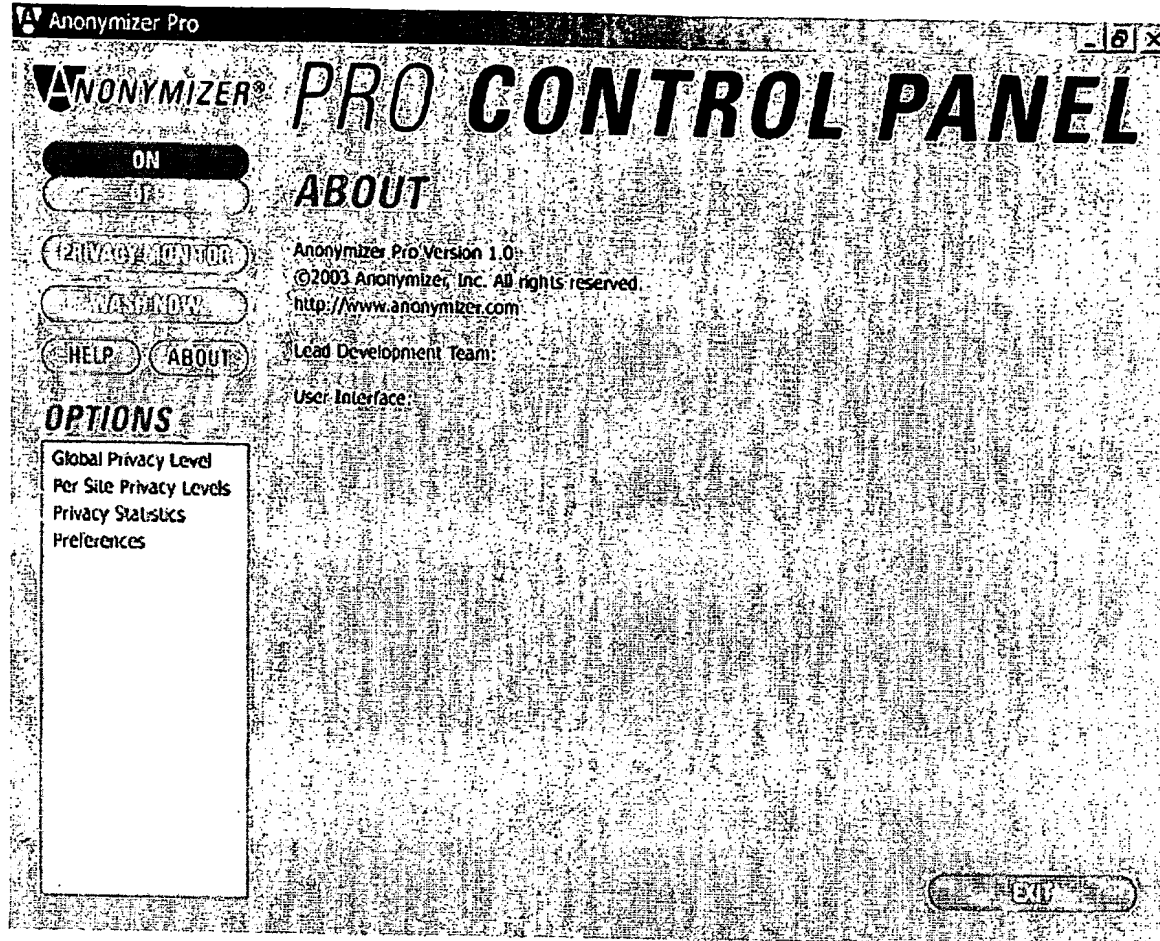


### 9.10.10. Help



Upon clicking on the help button a new window will appear with the help contents displayed. The help contents are generated using standard Windows help system. The above image displays as an example the current way the filtergate application displays help. We would keep this method and just substitute the text for AnonPro text.

### 9.10.11. About



## 10. System

This section describes the system requirements and components of the AnonPro Client.

### Platform

This section describes the platform that the AnonPro Client needs to run on.

- Windows 98
- Windows NT
- Windows 2000
- Windows XP

### 10.1. Languages

This section describes any language specifications that are required.

- English (default and primary language the AnonPro Client runs in)
- *In future versions: Support for Unicode languages (Chinese, Japanese, etc) in future releases of the AnonPro client. Not a requirement in this version.*

## 10.2. Error Handling

An exception class shall be developed that enables developers to create meaningful errors for help in debugging and troubleshooting.

## 10.3. Logging

Logging will need to be configurable and displayed to different outputs. The different outputs that should be supported are the Operating systems native event logging mechanism, the console and a file. The different levels of logging will be from 0-5 where 1 is display all messages and 5 displaying only critical messages, and 0 = no logging.

## 10.4. Reliability / Redundancy

### Security

To make communication as secure as required for the client, the product has two levels of end user access security. In the AnonPro Client, there are the following security components:

- 1 Application Layer Security
- 2 Network Security
- 3 Data archival and data classification

### Software Layer Security

At the heart of security is the need to establish the trust relationship between the users and the products servers (Anonymizer Proxy, Anonymizer Web-Server) to grant access privilege and subsequent ability to protect the transactions. Various security means are used to assure recipients that message comes from a sender whose identity is validated and that its contents have not been tampered with during the transmission.

- User-ID/Password Authentication
- SSL

## 10.5. Secure Session

Every product session is fully protected by using encryption technology. We use Secure Sockets Layer (SSL), which is widely adopted standard in industry, to encrypt data transmitted between a client and the <product> data center. 128-bit RC4 encryption mechanism in SSL is used to provide strong encryption.

For the web access application, you have to have a Web Browser that supports 128-bit SSL.

All the most popular Browsers support 128-bit SSL in recent versions.

## 10.6. Username and Password

Username and password is used in authentication, but password is not passed in clear over the network even though it is protected by SSL link. Instead, in AnonPro Client, it is hashed, and the resulting "digest" is then sent over the network. When it arrives at the server site, server checks it to against the saved digest on the server database.

## 11. Reference Documents

Title	Author	Date
AnonPro Functional Spec (this document)	James Reynolds	Draft 3
AnonPro Requirements Doc.	James Reynolds	Draft 2
AnonPro Proxy Support Functional Spec. Doc	Darya Mazandarany	Draft 1
AnonPro SSL-Server Functional Spec. Doc	Darya Mazandarany	Draft 1
AnonPro Web-Server Support Func. Spec. Doc	Gene Nelson	Draft 1
AnonWasher Functional Spec. Doc	Azi Sharif	Draft 1
AnonPro Test Plan	Azi Sharif	Draft 1

## 12. Glossary

### Product Acronyms

## Appendix A – Data Structure Definitions

### Preferences Bit Mask

This is a DWORD bit mask

Bit	feature
0	Pop up blocking
1	Ad Blocking
2	3rd party cookies
3	Web bugs
4	Ip hiding
5	Referer hiding
6	Page title hiding
7	Modify cookies
8	Os hiding
9	SSL fulltime
10	JavaScript Filtering
11	Active X Filtering
12	Java Filtering
13	VB Script Filtering
14	Active X Blocking
15	Block Cookies
16	Java Blocking
17	JavaScript Blocking
18	Blinking Text Blocking
19	Background music blocking
20 – 30	RESERVED
31	Blocked (new from Steve)

Please note: Bit 31 is being used as the "blocked" flag.

### APAuth Cookie

```
<APAuth>
  <tos>type of service</tos>
  <uname>encrypted user name</uname>
  <expires>unix timestamp for expiration</expires>
  <hash>hash of sec. String + tos + uname + expires + sec.
String</hash>
</APAuth>
```

## Meta-Auth Cookie

```
<APMeta-Auth>
  <uname>encrypted user name</uname>
  <uid>user id</uid>
</APMeta-Auth>
```

## AnonPro cookie

Sent with every request.

```
<anonpro>
<hash_reg>hash of the registration key MD5</hash_reg>
</anonpro>
```

## Blocked/Trusted/Protected List

This is the list format that we will use in the registry for these lists

```
<list>
  <version></version>
  <site>
    <domain></domain>
    <prefs></prefs>
    <modified>0||1</modified>
    <deleted>0||1 notifies us that the user has
    deleted this</deleted>
    <hardcoded>0||1 notifies us that this cannot be
    changed or deleted</hardcoded>
  </site>
</list>
```

## Server List

```
<list>
  <version></version>
  <server>
    <proxy>10.10.10.21</proxy>
    <proxy>10.10.10.22</proxy>
    <web>10.10.10.16</web>
    <web>10.10.10.17</web>
  </server>
</list>
```



## Update list

```
<list>
  <list_name>list_name</list_name>
  <version>version nbr</version>
  <server>
    <proxy>proxy ip</proxy>

    <web>web ip</web>
  </server>

  <site_list>
    <site>
      <domain>yahoo.com</domain>
      <hardcoded>0||1</hardcoded>
      <prefs>DWORD decimal with security settings</prefs>
    </site>

    <site>
      same as above
    </site>
  </site_list>
</list>
```

## Account\_Creation\_URL return

```
<root>
  <regval>
    <keystatus>invalid||used||new</keystatus>
    <publickey>public key generated by
server</publickey>
    <edition>ProductType</edition>
  </regval>
  <createacct>
    <account_status>invalid_uname||invalid_passwd||no
t_authorized||not_available||success</createacct>
    <suggestion_list>
      <suggestion>uname suggestion</suggestion>
    </suggestion_list>
    <uname>user name</uname>
    <enc_passwd>encrypted passwd</enc_passwd>
  </createacct>
  <error>invalid_action||none</error>
</root>
```

## Login\_URL return

<root>

<status>invalid||expired||inactive||active</status>

</root>

note if successful APAuth and APMeta-Auth will be set.

## Appendix B – Registry Settings

Root Key	Registry Name	Section used	Valid Values	Data Type	Syntax	Notes
HKCU	<b>Auto update</b>	Startup/init, Auth	0/1	Dword	Binary	0 = off, 1 = on In the preferences settings GUI, the user can select whether he/she will be notified of an auto-update of lists and binaries. During Authorization, the Web-Server will check to see if any new files are available for uploading to the client. If so, these files will be uploaded to the client. NOTE: This only happens if the user has selected this option as ON.
HKCU	<b>Auto_login</b>	Startup/init, Auth	0/1	Dword	Binary	0 = don't remember me, 1 = remember me In the preferences settings GUI, the user can select whether AnonPro logs the user in and authenticates the user with the Anonymizer Web-Server.
HKCU	<b>Auto_update_prompt</b>	Startup/init, Auth	0/1	Dword	Binary	0 = off, 1 = on In the preferences settings GUI, the user can select whether he/she will be prompted for new lists before they are automatically inserted.
HKCU\software\Microsoft\Windows\CurrentVersion\Run	<b>Run_when_windows_starts</b>	Startup/init	0/1	string	Path and name of the client executable.	0=off, 1=on In the preferences settings GUI, the user has the capability of specifying whether the AnonPro client should start automatically when windows start – or not.
HKCU	<b>Show_floater</b>	Startup/init, GUI	0/1	Dword	Binary	0=off, 1=on. In the preferences Settings GUI, the user has the capability to turn on the floaters.
HKCU	Dock_floater	Startup/init, GUI	0/1	Dword	Binary	0=dock, 1=nodock In the preferences settings GUI, the use has the capability to have the floaters docked at the

Root Key	Registry Name	Section used	Valid Values	Data Type	Syntax	Notes
						bottom of the screen of windows.
HKCU	<b>Default_state</b>	Startup/init, GUI	0/1	Dword	Binary	0=off, 1=on In the preferences settings GUI, the user has the capability to specify whether the client starts in "ON" mode or "OFF" mode.
HKCU	<b>Wash_on_Pro_Quit</b>	Startup/init, GUI	0/1	Dword	Binary	0=off, 1=on In the preferences settings GUI, the user has the capability to specify whether the AnonWasher should "wash" when the client is quit. Important note: If the client is turned off – then the wash is not performed. It is only if the client is quit. IMPORTANT: check if the client can catch a signal from windows when it is shutting down. Darya checked: the name of the sys.event is "AT_EXIT".
HKLM	<b>AnonWasher_Home</b>	GUI	Path	String	Path	This key has to be set by the AnonWasher installer. If not the AnonPro Installer will set this key instead. If the AnonWasher is already installed when the AnonPro Client is getting installed, then the AnonPro Client is NOT to override this value. This is the location of the anonwasher, which the "config washer" button points to and the "wash now" button points to. There is no option in the GUI to allow where the washer resides. By default, the Washer will reside in "c:\program files\anonymizer\anonwasher"
HKLM	<b>Referring_Hiding_Name</b>	Streaming	URL	String	URL	Name that is to be replaced as the "referrer" in for the referrer_hiding option.
HKLM	<b>OS_Hiding_Name</b>	Streaming	Win98, etc	String	Win98, Linux, etc	Name that is replaced when the OS_Hiding option is turned on.
HKLM	<b>Signup_URL</b>		URL	String		
HKLM	<b>Buy_Now_URL</b>	GUI				

Root Key	Registry Name	Section used	Valid Values	Data Type	Syntax	Notes
HKLM	<b>Login_URL</b>	Startup/init, Auth	URL	String	URL syntax	This is the URL that authenticates the userid and password that is either entered by the user or stored in the registry.
HKLM	<b>Update_URL</b>	Startup/init, Auth	URL	String	URL syntax	This is the URL of where all lists are pulled down.
HKLM	<b>Account_Creation_URL</b>	Startup/init (Wizard)	URL	String	URL syntax	After the reg.key has been validated (above), the user is rerouted to this URL for creating a new account.
HKLM	<b>Never_List_Redirect_URL</b>	Streaming	URL	String	URL	If the user types in a URL that is on the Neverlist, then they are redirected to this URL.
HKLM	<b>Never_List_Redirect_Image</b>	Streaming	Path/filename	String	Path	If the user loads a webpage which has images/banners that are from a never_list site, then load this image instead of the original image.
HKCU	<b>Anon_Pub_Key</b>	Startup/init, Auth	Key	String	Key format	Key used to validate all data coming from the Anon Web-Server.
HKLM	<b>AnonPro_Home Directory</b>	Startup/init, Auth	Path	String	Windows valid directory	Directory where AnonPro is stored.
CU	<b>Anon_Uname</b>	Startup/init, Auth	User name	String (already encrypted by server)	Valid user name from anon.	Encrypted user name sent back during startup wizard.
CU	<b>Anon_Password</b>	Startup/init, Auth	Password	String (already encrypted by server)	Valid password from anon web server	Encrypted password sent back during startup wizard.
CU	<b>Initial_Execution</b>	Startup/init	0/1	Dword	Binary	0=not yet run; 1=already run. Used to indicate if the wizard needs to run or has already run. During client installation, this needs to be set to 0 by the installer. After the "startup wizard" is run, the client has to be sure to change this flag to 1.
LM	HelpURL		URLName	String	URL valid name	
LM	<b>ServerList</b>		IP Addresses of our proxies	String (encrypted)	xml	List of proxy, and web ips
LM	<b>http_port</b>	TCP Hook	0-65000	Dword	Dword	

Root Key	Registry Name	Section used	Valid Values	Data Type	Syntax	Notes
LM	<b>https_port</b>	TCP Hook	0-65000	Dword	Dword	
CU	<b>TrustedList</b>		URL's	String (encrypted)	xml	
CU	<b>ProtectedList</b>		URL's	String (encrypted)	xml	
CU	<b>BlockedList</b>		URL's	String (encrypted)	xml	
CU	IFilters[Key]			Key (check if already encrypted. If not, then leave as is)		Filtergate settings as is.
HKLM	<b>ProductType</b>		Popup Shield, Cookie Shield, Privacy Monitor, Personal Web Shield	String	No comma's only single digit	Note: these settings will determine whether certain functionality is not activated (e.g. grayed out and unusable from the gui).
HKLM >microsoft	>>current_version Chooch_ProdType_Exp		Date	String (encrypted)	Date	This is to prevent users from reinstalling trial versions.
HKCU	<b>PagesBlocked</b>		0-999999	Dword		<same>
HKCU	<b>ActiveContentBlocked</b>		0-999999	Dword		<same>
HKCU	<b>AdsBlocked</b>		0-999999	Dword		<same>
HKCU	<b>PopupsBlocked</b>		0-999999	Dword		<same>
HKCU	<b>Security_Level</b>		1 of 7 bitmasks	Dword		This will be the bitmask corresponding to the security level that was selected using the slider. These bitmasks will be consts.

## Appendix C – Color RGB Matrix

Color Name	RGB Value
Red	Tbd.
Green	
Gray	
Yellow	
Dark Red	
Dark Gray	
Blue	
Dark Blue	

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US04/020562

International filing date: 25 June 2004 (25.06.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US  
Number: 60/483,277  
Filing date: 25 June 2003 (25.06.2003)

Date of receipt at the International Bureau: 06 December 2004 (06.12.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**